Dokumente
zu Datenschutz
und Informationsfreiheit
2008

Impressum

Herausgeber: **Berliner Beauftragter für Datenschutz und Informationsfreiheit**
An der Urania 4 – 10
10787 Berlin
Telefon: 0 30/1 38 89-0
Telefax: 0 30/2 15 50 50
E-Mail: mailbox@datenschutz-berlin.de
Internet: http://www.datenschutz-berlin.de

Druck: Brandenburgische Universitätsdruckerei und Verlagsgesellschaft mbH

Stand: Januar 2009

Inhaltsverzeichnis

Vorwort

Dieser Dokumentenband erscheint im 11. Jahr und fasst erneut alle Entschließungen und Stellungnahmen zusammen, die die Datenschutzbeauftragten und Aufsichtsbehörden in Deutschland, in Europa und auf internationaler Ebene in dieser Zeit verabschiedet haben. Die wachsende Zahl dieser Dokumente entspricht der zunehmenden Bedeutung von Datenschutz und Informationsfreiheit in der modernen Informationsgesellschaft. Auch wenn einige der Forderungen und Empfehlungen nicht umgesetzt worden sind, macht das breite Themenspektrum deutlich, dass sich die Beauftragten für Datenschutz und Informationsfreiheit vielen aktuellen Herausforderungen stellen und auf diesem Weg sowohl kontroverse Gesetzgebungsvorhaben kritisch begleiten als auch technische Entwicklungen so frühzeitig zu beeinflussen suchen, dass die Autonomie des Einzelnen gewahrt bleibt.

Hervorzuheben ist insbesondere die bei der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschlossene Berliner Erklärung, in der die Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts genannt werden. Zugleich wird die Bedeutung des Grundrechts auf Datenschutz für das Gemeinwohl in einer demokratischen Gesellschaft betont und sein Schutz als gesamtgesellschaftliche Aufgabe beschrieben. Dazu zählt auch die Stärkung von Medienkompetenz und Datenschutzbewusstsein gerade in der jungen Generation. Die Datenschutzbeauftragten haben zudem auf die zahlreichen Skandale im Bereich des Adresshandels und des Umgangs mit Kontodaten durch mehrere Entschließungen reagiert, die den Gesetzgeber zu entschlossenem Handeln aufgerufen haben.

Die datenschutzkonforme Gestaltung sozialer Netzwerke beschäftigte sowohl die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation als auch den Düsseldorfer Kreis der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, die beide hierzu detaillierte Stellungnahmen verfassten. Auch Internet-Portale zur Bewertung von Einzelpersonen und online abrufbare digitale Straßenansichten beschäftigten den Düsseldorfer Kreis.

Die Gruppe der europäischen Datenschutzbehörden (sog. Artikel 29-Gruppe) beschloss eine Stellungnahme zu Suchmaschinen, die auf Vorarbeiten der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation unter dem Vorsitz des Berliner Beauftragten für Datenschutz und Informationsfreiheit beruht. Auch die Frage, wie die Dopingbekämpfung datenschutzgerecht gestaltet werden kann, führte zu einer Stellungnahme der europäischen Datenschutzbehörden.

Die Informationsfreiheitsbeauftragten in Deutschland, deren Zahl erfreulicherweise steigt, befassten sich mit dem geringen Transparenzniveau in der Finanzverwaltung, aber auch mit gegenläufigen Entwicklungen bei der Informationsfreiheit auf europäischer Ebene.

Aufgabe der Beauftragten für Datenschutz und Informationsfreiheit ist es nicht nur, für eine Anwendung der hierfür geltenden Gesetze zu sorgen, sondern sich auch öffentlich für eine Stärkung dieser beiden Grundrechte einzusetzen. Diese Dokumentensammlung zeigt, wie ernst sie diese Aufgabe nehmen.

Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit

A. Dokumente zum Datenschutz

I. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1. Entschließungen der 75. Konferenz vom 3./4. April 2008 in Berlin

Berliner Erklärung:
Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts

Regelungen insbesondere zum großen Lauschangriff, zur Telekommunikationsüberwachung, zur Rasterfahndung, zur Online-Durchsuchung, zur automatischen Auswertung von Kfz-Kennzeichen und zur Vorratsspeicherung von Telekommunikationsdaten haben die verfassungsrechtlich zwingende Balance zwischen Sicherheitsbefugnissen der staatlichen Behörden und persönlicher Freiheit der Bürgerinnen und Bürger missachtet. Das Bundesverfassungsgericht hat mit einer Reihe von grundlegenden Entscheidungen diese Balance wieder hergestellt und damit auch den Forderungen der Datenschutzbeauftragten des Bundes und der Länder größtenteils Rechnung getragen.

Die Herausforderungen für den Datenschutz gehen aber weit über die genannten Bereiche hinaus. Datenverarbeitungssysteme dringen immer stärker in alle Lebensbereiche ein und beeinflussen den Alltag. Das Internet ist zum Massenmedium geworden. Vielfältig sind dabei die Möglichkeiten, das persönliche Verhalten zu registrieren und zu bewerten. Der nächste Quantensprung der Informationstechnik steht unmittelbar bevor: Die Verknüpfung von Informationstechnik mit Körperfunktionen, insbesondere bei der automatisierten Messung medizinischer Parameter und bei der Kompensation organischer Beeinträchtigungen. Die Miniaturisierung von IT-Systemen geht so weit, dass demnächst einzelne Komponenten nicht mehr mit bloßem Auge wahrgenommen werden können (Nanotechnologie).

Das Handeln staatlicher und nicht-öffentlicher Stellen ist verstärkt darauf gerichtet, viele Daten ohne klare Zweckbestimmung zu sammeln, um sie anschließend vielfältig auszuwerten, beispielsweise um versteckte Risiken aufzudecken oder um persönliches Verhalten unbemerkt zu beeinflussen. Geht es der Wirtschaft etwa darum, durch Scoringverfahren die Kundinnen und Kunden vorab einzuschätzen, gewinnt die immer exzessivere Registrierung und automatisierte Beob-

achtung für staatliche Stellen an Bedeutung. In beiden Bereichen wird ganz normales Verhalten registriert, unabhängig von konkreten Gefahren oder Verdachtsmomenten. Auch diejenigen, die sich nichts haben zu schulden kommen lassen, werden einem verstärkten Kontroll- und Anpassungsdruck ausgesetzt, der Einschüchterungseffekte zur Folge haben wird.

Der Schutz der Grundrechte, nicht zuletzt des Datenschutzes, dient in einer demokratischen Gesellschaft auch dem Gemeinwohl und ist zunächst Aufgabe jeglicher Staatsgewalt. Darüber hinaus ist er eine gesamtgesellschaftliche Aufgabe. Schließlich ist jede Bürgerin und jeder Bürger auch zur Eigenverantwortung aufgerufen. Hilfen zum informationellen Selbstschutz müssen zur Verfügung gestellt werden, die es den Betroffenen ermöglichen, eine Erfassung ihres Verhaltens zu vermeiden und selbst darüber zu entscheiden, ob und wem gegenüber sie Daten offenbaren. Von zunehmender Bedeutung sind auch Projekte, die das Datenschutzbewusstsein fördern, um vor allem jüngere Menschen von einem fahrlässigen Umgang mit ihren persönlichen Daten abzuhalten.

Alle diese Maßnahmen tragen zur Entwicklung einer neuen Datenschutzkultur bei. Voraussetzung dafür ist auch, dass nicht länger versucht wird, die verfassungsrechtlichen Grenzen und Spielräume auszureizen. Stattdessen muss dem Gebot der Datenvermeidung und -sparsamkeit Rechnung getragen werden.

Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten

1. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass das Bundesverfassungsgericht die Regelung zur Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen für nichtig erklärt hat. Hervorzuheben ist die Feststellung des Gerichts, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. 25 Jahre nach dem Volkszählungsurteil hat das Bundesverfassungsgericht damit den Datenschutz verfassungsrechtlich weiter gestärkt und ihn an die Herausforderungen des elektronischen Zeitalters angepasst.

2. Ein solches Grundrecht nimmt auch den Staat in die Verantwortung, sich aktiv für die Vertraulichkeit und Integrität informationstechnischer Systeme einzusetzen. Das Bundesverfassungsgericht verpflichtet den Staat, im Zeitalter der elektronischen Kommunikation Vertraulichkeit zu gewährleisten. Nunmehr ist der Gesetzgeber gehalten, diesen Auftrag konsequent umzusetzen. Dazu müssen die Regelungen, welche die Bürgerinnen und Bürger vor einer „elektronischen Ausforschung“ schützen sollen, gemäß den Vorgaben des Gerichts insbesondere im Hinblick auf technische Entwicklungen verbessert werden. Hier-

mit würde auch ein wesentlicher Beitrag geleistet, Vertrauen in die Sicherheit von E-Government- und E-Commerce-Verfahren herzustellen.

3. Die Konferenz unterstützt die Aussagen des Gerichts zum technischen Selbstschutz der Betroffenen. Ihre Möglichkeiten, sich gegen einen unzulässigen Datenzugriff zu schützen, etwa durch den Einsatz von Verschlüsselungsprogrammen, dürfen nicht unterlaufen oder eingeschränkt werden.

4. Die Konferenz begrüßt außerdem, dass das Bundesverfassungsgericht das neue Datenschutzgrundrecht mit besonders hohen verfassungsrechtlichen Hürden vor staatlichen Eingriffen schützt. Sie fordert die Gesetzgeber in Bund und Ländern auf, diese Eingriffsvoraussetzungen zu respektieren. Die Konferenz spricht sich in diesem Zusammenhang gegen Online-Durchsuchungen durch die Nachrichtendienste aus.

5. Das Bundesverfassungsgericht hat den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung auch bei Eingriffen in informationstechnische Systeme zu gewährleisten. Unvermeidbar erhobene kernbereichsrelevante Inhalte sind unverzüglich zu löschen. Eine Weitergabe oder Verwertung dieser Inhalte ist auszuschließen.

6. Auch wenn Online-Durchsuchungen innerhalb der durch das Bundesverfassungsgericht festgelegten Grenzen verfassungsgemäß sind, fordert die Konferenz die Gesetzgeber auf, die Erforderlichkeit von Online-Durchsuchungsbefugnissen kritisch zu hinterfragen. Sie müssen sich die Frage stellen, ob sie den Sicherheitsbehörden entsprechende Möglichkeiten an die Hand geben wollen. Die Konferenz bezweifelt, dass dieser weiteren Einbuße an Freiheit ein adäquater Gewinn an Sicherheit gegenüber steht.

7. Sollten gleichwohl Online-Durchsuchungen gesetzlich zugelassen werden, sind nicht nur die vom Bundesverfassungsgericht aufgestellten verfassungsrechtlichen Hürden zu beachten. Die Konferenz hält für diesen Fall zusätzliche gesetzliche Regelungen für erforderlich. Zu ihnen gehören vor allem folgende Punkte:

   – Soweit mit der Vorbereitung und Durchführung von Online-Durchsuchungen der Schutzbereich von Art. 13 GG (Unverletzlichkeit der Wohnung) betroffen ist, bedarf es dafür jedenfalls einer besonderen Rechtsgrundlage.

   – Der vom Bundesverfassungsgericht geforderte Richtervorbehalt ist bei Online-Durchsuchungen mindestens so auszugestalten wie bei der akustischen Wohnraumüberwachung. Ergänzend zu einer richterlichen Vorabkontrolle ist eine begleitende Kontrolle durch eine unabhängige Einrichtung vorzuschreiben.

- Gesetzliche Regelungen, welche Online-Durchsuchungen zulassen, sollten befristet werden und eine wissenschaftliche Evaluation der dabei gewonnenen Erkenntnisse und Erfahrungen anordnen.

- Informationstechnische Systeme, die von zeugnisverweigerungsberechtigten Berufsgruppen genutzt werden, sind von heimlichen Online-Durchsuchungen auszunehmen.

- Für die Durchführung von „Quellen-Telekommunikationsüberwachungen", die mit der Infiltration von IT-Systemen einhergehen, sind die gleichen Schutzvorkehrungen zu treffen wie für die Online-Durchsuchung selbst.

8. Schließlich sind die Gesetzgeber in Bund und Ländern aufgrund der Ausstrahlungswirkung der Entscheidung des Bundesverfassungsgerichts gehalten, die sicherheitsbehördlichen Eingriffsbefugnisse in Bezug auf informationstechnische Systeme, z. B. bei der Überwachung der Telekommunikation im Internet sowie der Beschlagnahme und Durchsuchung von Speichermedien, grundrechtskonform einzuschränken.

Mehr Augenmaß bei der Novellierung des BKA-Gesetzes

Der vom Bundesministerium des Innern erarbeitete Referentenentwurf eines Gesetzes zur Abwehr des internationalen Terrorismus durch das Bundeskriminalamt hat zum Ziel, das Bundeskriminalamt mit umfassenden polizeilichen Befugnissen zur Verhütung von terroristischen Straftaten und zur Abwehr von Gefahren für die öffentliche Sicherheit in diesem Zusammenhang auszustatten. Insbesondere sind Befugnisse zur Durchsuchung, Rasterfahndung, Wohnraumüberwachung und Telekommunikationsüberwachung vorgesehen. Außerdem will das Bundesinnenministerium eine Befugnis zum heimlichen Zugriff auf informationstechnische Systeme („Online-Durchsuchung") in das BKA-Gesetz aufnehmen.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dagegen aus, dass dem Bundeskriminalamt nach dem Gesetzentwurf mehr Befugnisse eingeräumt werden sollen, als einzelnen Landespolizeien zur Erfüllung ihrer eigenen Gefahrenabwehraufgaben zustehen. Sie halten es daher für geboten, im weiteren Gesetzgebungsverfahren die Befugnisse des BKA auf die zur Aufgabenerfüllung zwingend notwendigen Kompetenzen zu beschränken.

Die bisherige informationelle Gewaltenteilung zwischen den Polizeien der Länder und dem BKA diente auch dem Datenschutz. Die Konferenz fordert deshalb eine klare, d. h. hinreichend trennscharfe Abgrenzung der spezifischen Befug-

nisse des Bundeskriminalamts einerseits zu denen der Landespolizeien und Verfassungsschutzbehörden andererseits.

Dem Referentenentwurf zufolge soll die Aufgabenwahrnehmung durch das Bundeskriminalamt die Zuständigkeit der Landespolizeibehörden auf dem Gebiet der Gefahrenabwehr unberührt lassen. Dies führt zu erheblichen datenschutzrechtlichen Problemen, da nach geltendem Recht auch die Länder bei Abwehr einer durch den internationalen Terrorismus begründeten Gefahr parallele Abwehrmaßnahmen ergreifen können. Angesichts der Weite der für das Bundeskriminalamt vorgesehenen und den Landespolizeibehörden bereits eingeräumten Datenerhebungs- und Datenverarbeitungsbefugnisse steht zu befürchten, dass es zu sich überlappenden und in der Summe schwerwiegenderen Eingriffen in das informationelle Selbstbestimmungsrecht Betroffener durch das Bundeskriminalamt und die Landespolizeibehörden kommen wird.

Ebenso stellt sich die grundsätzliche Frage der Abgrenzung von Polizei und Verfassungsschutz. In den vergangenen Jahren sind die Polizeigesetze des Bundes und der Länder zunehmend mit Befugnissen zur verdeckten Datenerhebung (z. B. heimliche Video- und Sprachaufzeichnungen, präventive Telekommunikationsüberwachung) ausgestattet worden. Zudem wurden die Eingriffsbefugnisse immer weiter ins Vorfeld von Straftaten und Gefahren erstreckt. Damit überschneiden sich die polizeilichen Ermittlungsbefugnisse zunehmend mit denen des Verfassungsschutzes.

Das Bundesverfassungsgericht hat in seinem Urteil zur „Online-Durchsuchung“ vom 27.02.2008 den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung zu gewährleisten. Diese Vorgabe des Gerichts gilt nicht nur für eine etwaige gesetzliche Regelung zur „Online-Durchsuchung“, sondern für alle Eingriffsmaßnahmen. Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber deshalb auf, im Rahmen der Novellierung des BKA-Gesetzes den Schutz des Kernbereichs privater Lebensgestaltung für alle Eingriffsmaßnahmen zu regeln.

Keine Vorratsspeicherung von Flugpassagierdaten

Die EU-Kommission hat den Entwurf eines Rahmenbeschlusses des Rates zur Speicherung von Flugpassagierdaten und zu deren Weitergabe an Drittstaaten vorgelegt. Künftig sollen die Fluggesellschaften bei Flügen aus der EU und in die EU zu jedem Fluggast insgesamt 19 Datenelemente, bei unbegleiteten Minderjährigen sechs weitere Datenelemente, an eine von dem jeweiligen Mitgliedstaat bestimmte „Zentralstelle“ übermitteln. Die Daten sollen bei den Zentralstellen anlass- und verdachtsunabhängig insgesamt 13 Jahre lang personenbezogen ge-

speichert werden und zur Durchführung von Risikoanalysen dienen. Unter im Einzelnen noch unklaren Voraussetzungen sollen die Daten an Strafverfolgungsbehörden von Nicht-EU-Staaten (z. B. die USA) übermittelt werden dürfen. Neben Grunddaten zur Person, über Reiseverlauf, Buchungs- oder Zahlungsmodalitäten und Sitzplatzinformationen sollen auch andere persönliche Angaben gespeichert werden. Unklar ist, welche Daten unter „allgemeine Hinweise" gespeichert werden dürfen. Denkbar wäre, dass beispielsweise besondere Essenswünsche erfasst werden.

Mit der beabsichtigten Vorratsspeicherung und der Datenübermittlung wird die EU es auswärtigen Staaten ermöglichen, Bewegungsbilder auch von EU-Bürgerinnen und -Bürgern zu erstellen. In Zukunft besteht die Gefahr, dass Menschen Angst haben werden, durch ihre Reisegewohnheiten aufzufallen.

Die in dem Rahmenbeschluss vorgesehene Vorratsdatenspeicherung von Daten sämtlicher Fluggäste, die EU-Grenzen überschreiten, verstößt nicht nur gegen Art. 8 der Europäischen Menschenrechtskonvention und die Europaratskonvention 108, sondern ist auch mit dem im Grundgesetz verankerten Recht auf informationelle Selbstbestimmung nicht vereinbar. Grundrechtseingriffe „ins Blaue hinein", also Maßnahmen ohne Nähe zu einer abzuwehrenden Gefahr sind unzulässig.

Der Vorschlag für den Rahmenbeschluss erfolgte, ohne den Nutzen der erst jüngst in nationales Recht umgesetzten Richtlinie 2004/82/EG[1], die bereits alle Beförderungsunternehmen verpflichtet, die Daten von Reisenden an die Grenzkontrollbehörden zu übermitteln, auszuwerten. Hinzu kommt, dass der Vorschlag kaum datenschutzrechtliche Sicherungen enthält. Er bezieht sich nur auf eine bisher nicht bestehende und im Entwurf mit Mängeln behaftete EU-Datenschutzregelung. Diese Mängel wirken sich dadurch besonders schwerwiegend aus, dass in den Drittstaaten ein angemessenes Datenschutzniveau nicht immer gewährleistet ist und eine Änderung dieser Situation auch in Zukunft nicht zu erwarten ist. Die EU-Kommission hat nicht dargelegt, dass vergleichbare Maßnahmen in den USA, in Kanada oder in Großbritannien einen realen, ernst zu nehmenden Beitrag zur Erhöhung der Sicherheit geleistet hätten. Sie hat die kritischen Stellungnahmen der nationalen und des Europäischen Datenschutzbeauftragten sowie der Art. 29-Datenschutzgruppe nicht berücksichtigt.

Die Konferenz fordert die Bundesregierung auf, den Entwurf abzulehnen. Sie teilt die vom Bundesrat geäußerten Bedenken an der verfassungsrechtlichen Zulässigkeit der Speicherung der Passagierdaten.

[1] 1 RL 2004/82 EG v. 29.4.2004 Amtsbl. L 261 (2004) S. 24 ff., Richtlinie über die Verpflichtung von Beförderungsunternehmen, Angaben über die Beförderten zu übermitteln

Unzureichender Datenschutz beim deutsch-amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beobachtet mit Sorge, dass die Datenschutzrechte der Bürgerinnen und Bürger im Rahmen der internationalen Zusammenarbeit der Sicherheitsbehörden immer häufiger auf der Strecke bleiben. Aktuelles Beispiel ist das am 11.3.2008 paraphierte deutschamerikanische Regierungsabkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität. Die Konferenz fordert Bundestag und Bundesrat auf, dem Abkommen solange nicht zuzustimmen, bis ein angemessener Datenschutz gewährleistet ist.

Mit dem Abkommen wurde ein gegenseitiger Online-Zugriff auf Fundstellendatensätze von daktyloskopischen Daten und DNA-Profilen im hit/no-hit-Verfahren nach dem Muster des Prümer Vertrages vereinbart. Zudem wurden dessen Regelungen über den Austausch personenbezogener Daten zur Verhinderung terroristischer Straftaten weitgehend übernommen. Eine Übertragung des als Bedingung für diese umfangreichen Zugriffs- und Übermittlungsbefugnisse im Prümer Vertrag geschaffenen Datenschutzregimes erfolgte jedoch nicht.

Die Voraussetzungen, unter denen ein Datenaustausch erlaubt ist, sind nicht klar definiert. Der Datenaustausch soll allgemein zur Bekämpfung von Terrorismus und schwerer Kriminalität möglich sein. Welche Straftaten darunter konkret zu verstehen sind, wird nicht definiert. Es erfolgt hier lediglich der Verweis auf das jeweilige nationale Recht. Damit trifft nach dem Abkommen die USA einseitig eine Entscheidung über die Relevanz der abgerufenen Daten.

Bevor in so großem Umfang zusätzliche Datenübermittlungen erlaubt werden, muss zunächst geklärt werden, warum die bisherigen Datenübermittlungsbefugnisse für die internationale Polizeizusammenarbeit mit den USA nicht ausreichen.

Für die weitere Verarbeitung aus Deutschland stammender Daten in den USA bestehen für die Betroffenen praktisch keine Datenschutzrechte. Das Abkommen selbst räumt den Betroffenen keine eigenen Rechte ein, sondern verweist auch hierzu auf die Voraussetzungen im Recht der jeweiligen Vertragspartei. In den USA werden aber Datenschutzrechte, wie sie in der Europäischen Union allen Menschen zustehen, ausschließlich Bürgerinnen und Bürgern der Vereinigten Staaten von Amerika und dort wohnenden Ausländerinnen und Ausländern gewährt. Anderen Personen stehen Rechtsansprüche auf Auskunft über die Verarbeitung der eigenen Daten, Löschung unzulässig erhobener oder nicht mehr erforderlicher Daten oder Berichtigung unrichtiger Daten nicht zu. Außerdem besteht in den USA keine unabhängige Datenschutzkontrolle. Vor diesem Hinter-

grund sind die im Abkommen enthaltenen weiten Öffnungsklauseln für die weitere Verwendung der ausgetauschten Daten sowie der Verzicht auf Höchstspeicherfristen aus datenschutzrechtlicher Sicht nicht akzeptabel.

Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung von Arbeitnehmerinnen und Arbeitnehmern

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Übermittlung polizeilicher und nachrichtendienstlicher Erkenntnisse an Arbeitgeber zur Überprüfung von Bewerberinnen und Bewerbern, Beschäftigten und Fremdpersonal (z. B. Reinigungskräfte) außerhalb gesetzlicher Grundlagen. In zunehmendem Maß bitten Arbeitgeber die Betroffenen, in eine Anfrage des Arbeitgebers bei der Polizei oder dem Verfassungsschutz zu etwaigen dort vorliegenden Erkenntnissen zu ihrer Person einzuwilligen. In anderen Fällen sollen die Betroffenen eine solche Auskunft („fremdbestimmte Selbstauskunft“) selbst einholen und ihrem Arbeitgeber vorlegen. Eine solche „Einwilligung des Betroffenen“ ist regelmäßig keine wirksame Einwilligung. Die Betroffenen sehen sich oftmals dem faktischen Druck des Wohlverhaltens zum Zwecke des Erhalts und der Sicherung des Arbeitsplatzes ausgesetzt.

Die gesetzliche Grundentscheidung, in einem „Führungszeugnis“ dem Arbeitgeber nur ganz bestimmte justizielle Informationen zu einer Person verfügbar zu machen, wird dadurch unterlaufen. Es stellt einen Dammbruch dar, wenn jeder Arbeitgeber durch weitere Informationen direkt oder indirekt an dem Wissen der Sicherheitsbehörden und Nachrichtendienste teilhaben kann. Die Übermittlung dieser Informationen an Arbeitgeber kann auch den vom Bundesarbeitsgericht zum „Fragerecht des Arbeitgebers“ getroffenen Wertentscheidungen widersprechen. Danach darf der Arbeitgeber die Arbeitnehmerinnen und Arbeitnehmer bei der Einstellung nach Vorstrafen und laufenden Ermittlungsverfahren fragen, wenn und soweit die Art des zu besetzenden Arbeitsplatzes dies erfordert.

Polizei und Nachrichtendienste speichern – neben den in ein „Führungszeugnis“ aufzunehmenden Daten – auch personenbezogene Daten, die in das Bundeszentralregister gar nicht erst eingetragen werden oder Arbeitgebern in einem „Führungszeugnis“ nicht übermittelt werden dürfen. Es stellt eine grundsätzlich unzulässige Durchbrechung des Zweckbindungsgrundsatzes dar, wenn ein Arbeitgeber diese Daten – über den Umweg über die Polizei oder einen Nachrichtendienst – für Zwecke der Personalverwaltung erhält. Dabei ist besonders zu beachten, dass polizeiliche oder nachrichtendienstliche Daten nicht zwingend gesicherte Erkenntnisse sein müssen, sondern oftmals lediglich Verdachtsmomente sind. Die Folgen von Missdeutungen liegen auf der Hand.

Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen

Elektronische Identitäten sind der Schlüssel zur Teilnahme an der digitalen Welt. Die Möglichkeiten der pseudonymen Nutzung, die Gewährleistung von Datensparsamkeit und -sicherheit und der Schutz vor Identitätsdiebstahl und Profilbildung sind wichtige Grundpfeiler moderner Informations- und Kommunikationstechnologien. Darauf hat die Bundesregierung zu Recht anlässlich des Zweiten Nationalen IT-Gipfels im Dezember 2007 (Hannoversche Erklärung) hingewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass der gesetzliche Rahmen für die anonyme oder pseudonyme Nutzung elektronischer Verfahren bereits seit langem vorhanden ist. Beispielsweise hat jeder Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 13 Abs. 6 Telemediengesetz).

Bisher werden jedoch anonyme oder pseudonyme Nutzungsmöglichkeiten nur sehr selten angeboten. Vielmehr speichern Wirtschaft und Verwaltung immer mehr digitale Daten mit direktem Personenbezug. Erschlossen werden diese Datenbestände in der Regel über einheitliche Identifizierungsnummern. Mit der lebenslang geltenden, bundeseinheitlichen Steuer-Identifikationsnummer (Steuer-ID) oder der mit der Planung der Gesundheitskarte zusammenhängenden, ebenfalls lebenslang geltenden Krankenversichertennummer werden derzeit solche Merkmale eingeführt. Auch mit der flächendeckenden Einführung des ePersonalausweises wird jeder Bürgerin und jedem Bürger eine elektronische Identität zugewiesen, mit der sie bzw. er sich künftig auch gegenüber eGovernment-Portalen der Verwaltung oder eCommerce-Angeboten der Wirtschaft identifizieren soll.

Einheitliche Personenkennzeichen bergen erhebliche Risiken für das Recht auf informationelle Selbstbestimmung. So könnte sich aus der Steuer-ID ein Personenkennzeichen entwickeln, über das alle möglichen Datenbestände personenbezogen verknüpft und umfassende Persönlichkeitsprofile erstellt werden. Angesichts der stetig verbesserten technischen Möglichkeiten, zunächst verteilt gespeicherte Daten anwendungsübergreifend zu verknüpfen, wachsen entsprechende Begehrlichkeiten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die effektive Nutzung von Informationstechnik und hohe Datenschutzstandards keinen Widerspruch bilden. Ein datenschutzförderndes Identitätsmanagement kann den Einzelnen vor unangemessener Überwachung und Verknüpfung seiner Daten schützen und zugleich eine moderne und effektive Datenverarbeitung ermöglichen. Entsprechende EU-Projekte wie PRIME (Privacy and Identity Management for Europe) und FIDIS (Future of Identity in the Infor-

mation Society) werden im Rahmen des 6. Europäischen Forschungsprogramms „Technologien für die Informationsgesellschaft“ gefördert.

Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren. Datenschutzfördernde Identitätsmanagementsysteme schließen Verknüpfungen nicht aus, wenn die Nutzenden es wünschen oder wenn dies gesetzlich vorgesehen ist. Sie verhindern jedoch, dass unkontrolliert der Bezug zwischen einer elektronischen Identität und einer Person hergestellt werden kann. Unter bestimmten, klar definierten Bedingungen kann mit Hilfe von Identitätsmanagementsystemen sichergestellt werden, dass ein Pseudonym bei Bedarf bezogen auf einen bestimmten Zweck (z. B. Besteuerung) einer Person zugeordnet werden kann.

Identitätsmanagementsysteme werden nur dann die Akzeptanz der Nutzerinnen und Nutzer finden, wenn sie einfach bedienbar sind, ihre Funktionsweise für alle Beteiligten transparent ist, möglichst alle Komponenten standardisiert sind und die Technik von unabhängigen Dritten jederzeit vollständig nachprüfbar ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung daher auf, den Absichtserklärungen des IT-Gipfels Taten folgen zu lassen und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben. Sowohl die öffentliche Verwaltung als auch die Wirtschaft sollte die Einführung solcher datenschutzfördernder Systeme unterstützen.

Medienkompetenz und Datenschutzbewusstsein in der jungen „online-Generation“

1. Die Nutzung moderner Informationssysteme ist auch mit Risiken verbunden. Diese begründen ein besonderes Schutzbedürfnis der Bürgerinnen und Bürger. Dieses verlangt aber nicht nur rechtliche Vorkehrungen und Sicherungen, sondern auch Aufklärung und Information darüber, mit welchen Risiken die Nutzung dieser Informationssysteme verbunden sind. Dies gilt vor allem für die junge „online- Generation“, die in der Altersgruppe der 14- bis 19-Jährigen zu 96 % regelmäßig das Internet nutzt und zwar im Durchschnitt länger als zweieinhalb Stunden täglich.

2. Die Datenschutzbeauftragten des Bundes und der Länder sehen es daher als wichtige Aufgabe an, Kinder und Jugendliche für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den Daten anderer zu sensibilisieren. Diese Aufgabe obliegt gesellschaftlichen Einrichtungen ebenso wie staatlichen Organen.

Die Erfahrungen, die anlässlich des 2. Europäischen Datenschutztages am 28. Januar 2008 gemacht wurden, stützen dies. Zu dem Motto „Datenschutz macht Schule“ wurde von den Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl von Veranstaltungen und Schulbesuchen organisiert. Eltern, Lehrkräfte, Schülerinnen und Schüler, aber auch Studierende hatten dabei die Möglichkeit, sich z. B. bei Podiumsdiskussionen, Rollenspielen und Workshops über datenschutzrelevante Fragen bei der Nutzung moderner Medien zu informieren. Die dabei gewonnenen Erfahrungen lassen nicht nur einen enormen Informationsbedarf, sondern auch ein großes Informationsinteresse erkennen, und zwar bei allen Beteiligten, bei den Jugendlichen ebenso wie bei ihren Eltern und den Lehrkräften.

Bei den Informationsangeboten, die derzeit den Schulen angeboten werden, um die Medienkompetenz junger Menschen zu verbessern, spielt das Thema „Datenschutz“ aber nur eine untergeordnete Rolle. Es beschränkt sich überwiegend auf Fragen der Datensicherheit und wird zudem häufig von Fragen des Jugendmedienschutzes und des Verbraucherschutzes überlagert.

3. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für notwendig, dass die für die schulische Bildung zuständigen Ministerinnen und Minister der Landesregierungen bei der Förderung der Medienkompetenz von Kindern und Jugendlichen – schon im Grundschulalter – deren Datenschutzbewusstsein stärken. Der Datenschutz muss bei den Angeboten und Projekten zur Förderung der Medienkompetenz eine größere Rolle spielen. Die bisherigen Ansätze reichen bei weitem nicht aus. Gerade bei jungen Menschen muss das Bewusstsein über den Datenschutz als Bürgerrecht und Bestandteil unserer demokratischen Ordnung stärker gefördert werden.

2. Entschließung zwischen der 75. und 76. Konferenz (vom 16. September)

Entschlossenes Handeln ist das Gebot der Stunde

Nie haben sich in der jüngeren Geschichte die Skandale um den Missbrauch privater Daten in der Wirtschaft so gehäuft wie heute und damit deutlich gemacht, dass nicht nur im Verhältnis Bürger – Staat das Grundrecht auf informationelle Selbstbestimmung bedroht ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt – zuletzt in ihrer Berliner Erklärung vom 4. April dieses Jahres – auf diese Gefahren hingewiesen, die von massenhaften

Datensammlungen privater Unternehmen und ihrer unkontrollierten Nutzung ausgehen. Sie hat auch deshalb den Gesetzgeber zu einer grundlegenden Modernisierung und Verbesserung des Datenschutzrechts aufgefordert und eine neue Datenschutzkultur angemahnt.

Dass jetzt endlich im politischen und gesellschaftlichen Raum die Problematik erkannt und diskutiert wird, ist zu begrüßen. Dabei kann und darf es aber nicht bleiben, nur entschlossenes Handeln kann die Bürgerinnen und Bürger vor weiterem Missbrauch ihrer persönlichen Daten schützen und das verlorene Vertrauen wiederherstellen.

Das vom Grundgesetz garantierte Recht eines Jeden, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu entscheiden, muss endlich die ihm gebührende Beachtung finden Die Weitergabe von persönlichen Angaben zu Werbezwecken darf nur mit ausdrücklicher Einwilligung der Betroffenen zulässig sein. Daten sind mit einem Vermerk über ihre Quelle zu kennzeichnen. Der Abschluss von Verträgen darf nicht von der Einwilligung in die Datenübermittlung zu Werbezwecken abhängig gemacht werden. Verstöße gegen den Datenschutz dürfen nicht ohne Konsequenzen bleiben, sondern müssen strikt geahndet werden. Deshalb müssen die bestehenden Lücken in den Bußgeld- und Strafbestimmungen geschlossen und der Bußgeld- und Strafrahmen für Datenschutzverstöße deutlich erhöht werden. Diese Sofortmaßnahmen, die bereits Gegenstand des Spitzentreffens im Bundesministerium des Innern am 4. September 2008 waren, können vom Deutschen Bundestag noch in den bereits vorliegenden Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes aufgenommen werden.

Gesetzgeberische Maßnahmen allein helfen aber nicht weiter, wenn ihre Einhaltung nicht ausreichend kontrolliert und Verstöße nicht sanktioniert werden können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, die Datenschutzaufsichtsbehörden endlich organisatorisch, personell und finanziell in die Lage zu versetzen, ihren Beratungs- und Kontrollaufgaben flächendeckend, unabhängig und wirkungsvoll nachkommen zu können, und entsprechend der EU-Datenschutzrichtlinie mit wirksamen Einwirkungsbefugnissen auszustatten, die sie bisher nicht haben.

Außerdem müssen Konzepte zur grundlegenden Modernisierung des Datenschutzes entwickelt und umgesetzt werden. Wichtige Themen sollten dabei noch in dieser Legislaturperiode angegangen werden:

– Verbesserung der Protokollierung des Datenzugriffs in automatisierten Verfahren

– Stärkung der datenschutzrechtlichen Auskunftsrechte

– Pflicht zur Information der betroffenen Personen und der Aufsichtsbehörden bei Datenpannen und missbräuchlicher Datennutzung

– Gewinnabschöpfung aus unbefugtem Datenhandel

– Einführung eines gesetzlich geregelten Datenschutzaudits, mit dem unabhängig und qualifiziert die Datenschutzkonformität von Verfahren und Produkten bestätigt wird

– Stärkung der betrieblichen Datenschutzbeauftragten als Organ der Selbstkontrolle

– Spezialisierung der Strafverfolgungsbehörden

– Anerkennung von Datenschutzbestimmungen als verbraucherschützende Normen.

Nur wenn jetzt den Ankündigungen Taten folgen und entschlossen gehandelt wird, können die Bürgerinnen und Bürger künftig vor Datenmissbrauch und Verletzung ihres Grundrechts auf informationelle Selbstbestimmung besser als in der Vergangenheit geschützt werden.

3. Entschließungen der 76. Konferenz vom 6./7. November 2008 in Bonn

Mehr Transparenz durch Informationspflichten bei Datenschutzpannen

In den letzten Monaten hat eine Reihe von gravierenden Datenschutzverstößen die Aufmerksamkeit der Öffentlichkeit und der Medien gefunden. In vielen dieser Fälle lag der Verlust oder Missbrauch personenbezogener Daten längere Zeit zurück und war der verantwortlichen Stelle bekannt, ohne dass die Betroffenen oder die zuständige Datenschutzaufsichtsbehörde hierüber informiert worden wären. Dadurch wurde ihnen die Möglichkeit genommen, Sicherheitsmaßnahmen zu ergreifen und mögliche Schäden zu begrenzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt deswegen die Forderung, alle verantwortlichen Stellen – grundsätzlich auch alle öffentlichen Stellen – gesetzlich zu verpflichten, bei Verlust, Diebstahl oder Missbrauch personenbezogener Daten unverzüglich die hiervon betroffenen Bürgerinnen und Bürger und die zuständigen Aufsichts- oder Kontrollbehörden sowie gegebenenfalls auch die Öffentlichkeit zu unterrichten. Dies entspricht

ihrer datenschutzrechtlichen Verantwortung und ermöglicht es den Betroffenen, negative Konsequenzen solcher Datenschutzpannen abzuwenden oder einzugrenzen. Hinter diesem Interesse hat der Wunsch der entsprechenden Stellen zurückzustehen, solche Vorkommnisse geheim zu halten, um keinen Imageschaden oder keine wirtschaftlichen Nachteile zu erleiden.

Etliche Staaten haben bereits entsprechende Regelungen. Eine solche Informationspflicht würde die Transparenz erhöhen und das Vertrauen der Betroffenen in eine korrekte Datenverarbeitung stärken. Darüber hinaus würde sie einen wichtigen Anstoß geben, mehr für Datenschutz und Datensicherheit zu tun.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, entsprechende umfassende Informationspflichten für Unternehmen und öffentliche Stellen im Bundesdatenschutzgesetz und den Landesdatenschutzgesetzen zu schaffen. Die übrigen aus Anlass der Datenschutzskandale in einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16.09.2008 erläuterten Forderungen zur Novellierung des Bundesdatenschutzgesetzes werden bekräftigt.

Angemessener Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in der EU dringend erforderlich

Auf europäischer Ebene ist eine Vielzahl von Vorhaben beschlossen bzw. initiiert worden, die in ihrer Gesamtheit zu erheblichen Eingriffen in die Persönlichkeitsrechte führt:

- Die Telekommunikationsunternehmen in den Mitgliedstaaten der EU sind verpflichtet, die bei der Nutzung öffentlich zugänglicher Telekommunikationsdienste anfallenden Verkehrsdaten über das Kommunikationsverhalten der Einzelnen für die Sicherheitsbehörden ohne konkreten Anlass auf Vorrat zu speichern.

- Die Pässe der Bürgerinnen und Bürger der EU-Mitgliedstaaten werden mit biometrischen Merkmalen ausgestattet.

- Fluggastdaten (PNR) werden in die USA übermittelt, um sie den dortigen Behörden zur Verfügung zu stellen. Die Nutzung von Fluggastdaten zu Strafverfolgungszwecken wird auch in der Europäischen Union vorbereitet.

- Der Vertrag von Prüm, der in den Rechtsrahmen der Union überführt wird, ermöglicht den Polizei- und Strafverfolgungsbehörden der Mitgliedstaaten einen gegenseitigen Zugriff auf Fingerabdruck-, DNA- und Kfz-Daten.

- Es soll ein Europäisches Strafregisterinformationssystem geschaffen werden, mit dem Informationen über strafrechtliche Verurteilungen zwischen den Mitgliedstaaten ausgetauscht werden können.

- Das Schengener Informationssystem wird weiter ausgebaut, u. a. durch die Speicherung von biometrischen Merkmalen. Zudem wird der Kreis der Nutzer erweitert um das Europäische Polizeiamt EUROPOL und die Einheit für justizielle Zusammenarbeit in der EU (EUROJUST).

- Ein Europäisches Visa-Informationssystem (VIS) wird eingeführt, um den Austausch von Visa-Daten zwischen den Mitgliedstaaten zu erleichtern. Auch für EUROPOL, die Sicherheitsbehörden und die Nachrichtendienste soll dieser Datenbestand zugänglich sein.

- Das europäische Verfahren EURODAC, in dem die Fingerabdrücke von Asylbewerberinnen und Asylbewerbern gespeichert sind, soll auch von der Polizei und den Strafverfolgungsbehörden genutzt werden können.

- Der Aufgabenbereich von EUROPOL soll über die Bekämpfung der Organisierten Kriminalität hinaus auch auf andere Formen der schweren Kriminalität erweitert werden. Außerdem soll EUROPOL erstmals die Befugnis erhalten, Daten auch von privaten Stellen entgegenzunehmen und Zugriff auf alle polizeilich relevanten Datenbanken in der EU bekommen.

- Der Informationsaustausch zwischen den Strafverfolgungsbehörden der EU wird entsprechend dem Rahmenbeschluss des Rates vom 18. Dezember 2006 („Schwedische Initiative“) ausgebaut. Danach soll der Austausch verfügbarer Daten innerhalb der EU zu den gleichen Bedingungen erfolgen wie nach nationalem Recht.

Neben diesen Vorhaben gibt es zudem Abkommen auf bilateraler Ebene zwischen EU-Mitgliedstaaten und Drittstaaten, wie z. B. das Abkommen der Bundesrepublik Deutschland mit den Vereinigten Staaten für einen erweiterten Informationsaustausch zwischen den Sicherheitsbehörden.

Der Aufbau zentraler Datenbestände und der Ausbau der grenzüberschreitenden Datenübermittlung greifen erheblich in das Grundrecht auf informationelle Selbstbestimmung ein und führen dadurch zu Gefahren für jede Einzelne und jeden Einzelnen. Diese werden noch gesteigert durch die angestrebte Verknüpfbarkeit der bestehenden und geplanten Datenbanken.

Umso wichtiger ist deshalb ein hoher und gleichwertiger Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Europa. Dies wurde von den Datenschutzbeauftragten auf nationaler und europäischer Ebene mehrfach ange-

mahnt. Der hierzu im Oktober 2005 vorgelegte Rahmenbeschluss-Vorschlag genügt diesen Anforderungen nicht (siehe dazu die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 „Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen"). Zur Wahrung des erforderlichen Gleichgewichts zwischen Freiheit und Sicherheit sollten die Parlamente und Regierungen ihre Einflussmöglichkeiten bei europäischen Vorhaben stärker nutzen und dabei auch datenschutzrechtliche Aspekte einbringen. Wie notwendig ein angemessener Datenschutz ist, hat sich beim Verfahren der Aufnahme Verdächtiger in die so genannte EU-Terrorliste gezeigt, das durch den Europäischen Gerichtshof für rechtswidrig erklärt wurde.

Die Datenschutzbeauftragten fordern deshalb:

– Bei jeder neuen Initiative ist das Verhältnismäßigkeitsprinzip zu wahren und deren Auswirkung auf das bestehende System von Eingriffsmaßnahmen zu berücksichtigen.

– Im Hinblick auf den Kumulationseffekt sind die verschiedenen europäischen Initiativen zudem grundrechtskonform aufeinander abzustimmen. Redundanzen und Überschneidungen müssen verhindert werden.

– Ein Rechtsakt muss unverzüglich beschlossen werden, der über den Rahmenbeschlussvorschlag hinaus einen hohen und gleichwertigen Datenschutzstandard bei der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit verbindlich vorschreibt. Die gesamte nationale und grenzüberschreitende Informationsverarbeitung in diesem Bereich muss davon erfasst sein, um ein einheitliches Datenschutzniveau in den EU-Mitgliedstaaten zu gewährleisten.

– Ein unabhängiges, beratendes Datenschutzgremium sowie eine unabhängige und umfassende datenschutzrechtliche Kontrolle müssen für die polizeiliche und justizielle Zusammenarbeit eingerichtet bzw. gewährleistet werden.

Besserer Datenschutz bei der Umsetzung der „Schwedischen Initiative" zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedstaaten geboten

Der Rahmenbeschluss des Rates zur Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten (sog. „Schwedische Initiative") vom 18.12.2006 verpflichtet diese, an die grenzüberschreitende Übermittlung personenbezogener Daten innerhalb der EU keine höheren Anforderungen zu stellen, als auf nationaler Ebene für den Datenaustausch zwischen

Polizei- und Strafverfolgungsbehörden gelten. Seine Umsetzung wird zu einem deutlichen Anstieg und zur Beschleunigung des Informationsaustausches und damit zu einer weiteren Intensivierung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen auf EU-Ebene führen. Das erstrebte Ziel, nämlich die Schaffung eines Raumes der Freiheit, der Sicherheit und des Rechts setzt aber auch voraus, dass in den Mitgliedstaaten ein möglichst gleichwertiger Datenschutz auf hohem Niveau besteht. Dies ist bislang nicht erfüllt. Es besteht nach wie vor der aus datenschutzrechtlicher Sicht unhaltbare Zustand, dass die auf EU-Ebene ausgetauschten polizeilichen Informationen in den jeweiligen EU-Mitgliedstaaten unterschiedlichen Datenschutzregelungen hinsichtlich ihrer Verwendung unterworfen sind. Zudem gelten keine einheitlichen Rechte auf Auskunft, Berichtigung und Löschung der Datenverarbeitung für die Betroffenen in den Empfängerstaaten.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, den bei der innerstaatlichen Umsetzung der „Schwedischen Initiative“ verbleibenden Spielraum zu nutzen und die Befugnisse zum Informationsaustausch mit den Strafverfolgungsbehörden der EU-Mitgliedstaaten für die nationalen Polizei- und Strafverfolgungsbehörden normenklar und unter Beachtung des Grundsatzes der Verhältnismäßigkeit gesetzlich zu regeln. Dazu zählen insbesondere:

– Ausschluss der gesonderten Erhebung der angefragten Daten durch die Strafverfolgungsbehörden allein um diese zu übermitteln.

– Eindeutige inhaltliche Anforderungen, die an ein Ersuchen um Datenübermittlung zu stellen sind, um Überschussinformationen zu vermeiden,

– Regelung enger Voraussetzungen für sog. Spontanübermittlungen, um für den Empfänger nutzlose und damit nicht erforderliche Übermittlungen auszuschließen,

– Nutzung des Spielraums bei der Ausgestaltung der Verweigerungsgründe, um unverhältnismäßige Datenübermittlungen zu verhindern,

– normenklare Abgrenzung der Befugnis zur Übermittlung von Daten zu präventiven Zwecken gegenüber der justiziellen Rechtshilfe,

– vollständige Umsetzung der Datenschutzbestimmungen in Art. 8 des Rahmenbeschlusses und begrenzende Regelungen zur Weiterübermittlung an Drittstaaten,

– normenklare Bestimmung welche Behörden als zuständige Strafverfolgungsbehörden im Sinne des Rahmenbeschlusses gelten und welche Informationen

nur durch Ergreifen von Zwangsmaßnahmen im Sinne des Rahmenbeschlusses verfügbar sind,

– normenklare Bestimmung, welche Informationen nicht vom Rahmenbeschluss erfasst werden, weil sie für die Strafverfolgungsbehörden nur durch das Ergreifen von Zwangsmaßnahmen verfügbar sind.

Datenschutzgerechter Zugang zu Geoinformationen

Die Einführung einer einheitlichen Geodateninfrastruktur und die Veröffentlichung der staatlichen Daten eröffnen ein großes Potential an volkswirtschaftlichem Nutzen und ist geeignet, vielen E-Government- und E-Commerce-Anwendungen die erforderliche Infrastruktur zur Verfügung zu stellen. Als einen ersten Schritt regelt das europäische Recht mit der so genannten INSPIRE-Richtlinie, die bis Mai 2009 in nationales Recht umgesetzt werden muss, die Bereitstellung von amtlichen Geodaten nach einheitlichen Standards für europaweite behördliche, kommerzielle und private Nutzungen.

Durch diese neue Infrastruktur werden georeferenzierbare Angaben auf Grund der Erschließungsmöglichkeit über Wohnanschriften oder Eigentümer- bzw. Standortdaten als personenbezogene Daten zur Verfügung gestellt. Diesem Umstand müssen die gesetzlichen Regelungen gerecht werden und angemessene Datenschutzregelungen enthalten.

Bei der Bereitstellung amtlicher Geodaten ist sowohl nach der europäischen Richtlinie als auch nach deutschem Verfassungsrecht der Schutz personenbezogener Daten angemessen zu gewährleisten. Der Entwurf der Bundesregierung zur Umsetzung dieser Richtlinie in einem Geodatenzugangsgesetz (BT-Drs. 16/10530) sieht eine entsprechende Anwendung der Schutzvorschriften des Umweltinformationsgesetzes vor. Im Gegensatz zum einzelfallbezogenen Zugang nach den Umweltinformationsgesetzen birgt der im Entwurf eines Geodatenzugangsgesetzes vorgesehene massenhafte Abruf solcher Daten aber ein höheres datenschutzrechtliches Gefährdungspotenzial. Der Verweis auf das Umweltinformationsgesetz ist nach Ansicht der Konferenzen der Datenschutz- und der Informationsfreiheitsbeauftragten des Bundes und der Länder deshalb nicht interessengerecht. Ein Geodatenzugangsgesetz muss einen differenzierenden Ausgleich zwischen Informations und Schutzinteressen für die spezielle Problematik der Geobasis- und der Geofachdaten vornehmen. Es ist insbesondere zu berücksichtigen, dass nach der INSPIRE-Richtlinie die Zugangsmöglichkeit eingeschränkt werden soll, wenn der Zugang nachteilige Auswirkungen auf die Vertraulichkeit personenbezogener Daten haben kann.

Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren

Die Bundesregierung hat am 25.06.2008 den Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen (BT-Drs. 16/10492). Danach haben Beschäftigte die monatliche Übermittlung ihrer Einkommensdaten an die Zentrale Speicherstelle zu dulden, obwohl zurzeit nicht verlässlich abgeschätzt werden kann, in welchem Umfang die Speicherung der Daten tatsächlich erforderlich ist. Ein großer Anteil der Betroffenen wird die dem Anwendungsbereich des ELENA-Verfahrens unterfallenden Sozialleistungen niemals oder erst zu einem erheblich späteren Zeitpunkt geltend machen. Es steht somit bereits jetzt zu vermuten, dass eine große Zahl der übermittelten Daten von der Zentralen Speicherstelle wieder zu löschen sein wird, ohne jemals für irgendein Verfahren genutzt worden zu sein.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb wiederholt verfassungsrechtliche Bedenken unter dem Gesichtspunkt der Verhältnismäßigkeit und speziell der Erforderlichkeit geltend gemacht und eine substantiierte Begründung gefordert. Diese ist nicht erfolgt. Bisher bestehen lediglich höchst vage Erwartungen auf langfristige Effizienzsteigerungen insbesondere der Arbeitsverwaltung. Angesichts dieser Unklarheiten verbleiben erhebliche Zweifel an der Verfassungsmäßigkeit des Gesetzes. Hinzu kommt, dass derartige umfangreiche Datensammlungen Begehrlichkeiten wecken, die Daten für andere Zwecke zu verwenden.

Für den Fall, dass diese verfassungsrechtlichen Bedenken ausgeräumt werden können, sind unter dem Gesichtspunkt des *technisch-organisatorischen Datenschutzes* noch folgende Verbesserungen durch den Gesetz- bzw. Verordnungsgeber erforderlich:

– Es muss sichergestellt werden, (z. B. durch die Einrichtung eines Verwaltungsausschusses der Zentralen Speicherstelle), dass unter Mitwirkung von Datenschutzbeauftragten gemeinsame Grundsätze zur Wahrung des Datenschutzes und der technischen Sicherheit berücksichtigt werden.

– Für die Zentrale Speicherstelle muss ein Datenschutzbeauftragter eingesetzt werden, der dazu verpflichtet ist, regelmäßig an den Verwaltungsausschuss zu berichten.

– Schlüssel zur Ver- und Entschlüsselung der bei der Zentralen Speicherstelle gespeicherten Daten dürfen nicht in der Verfügungsgewalt der Zentralen Speicherstelle liegen. Die Ver- und Entschlüsselungskomponente muss von einer unabhängigen Treuhänderstelle verantwortet werden.

– Mittelfristig ist ein Verfahren anzustreben, das die technische Verfügungsmöglichkeit über die individuellen Daten den Betroffenen überträgt.

– Das im Rahmen der ELENA-Modellvorhaben erarbeitete differenzierte Löschungskonzept muss weiterentwickelt und umgesetzt werden.

– Für abrufende Stellen sind starke Authentisierungsverfahren vorzuschreiben, die dem Stand der Technik entsprechen und den Forderungen der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren genügen.

– Für die technischen Komponenten muss eine Zertifizierung durch eine unabhängige Prüfung vorgeschrieben werden.

Abfrage von Telekommunikationsverkehrsdaten einschränken: Gesetzgeber und Praxis müssen aus wissenschaftlichen Erkenntnissen Konsequenzen ziehen

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Auftrag des Bundesministeriums der Justiz die Nutzung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung (§§ 100g, 100h StPO alte Fassung) evaluiert. Die Studie geht zu Recht davon aus, dass Verkehrsdaten ein hohes Überwachungspotential in sich tragen und besser als andere Daten dazu geeignet sind, soziale Netzwerke nachzuweisen, Beziehungen zu identifizieren und Informationen über Individuen zu generieren. Der Studie zufolge ist die Zahl der Verkehrsdatenabfragen erheblich und kontinuierlich von 10.200 (2002) auf 40.000 Abfragen (2005) angestiegen. Zudem erfasst die Maßnahme regelmäßig auch eine Vielzahl unbescholtener Bürgerinnen und Bürger.

Das Bundesministerium der Justiz hat die Studie erst im Februar dieses Jahres und somit nach der Neuregelung der Telekommunikationsüberwachung und Einführung der Vorratsdatenspeicherung veröffentlicht. Das Gutachten liefert Erkenntnisse, deren Berücksichtigung im Gesetz vom 21. Dezember 2007 erforderlich gewesen wäre. Die Datenschutzbeauftragten des Bundes und der Länder sehen sich durch die Studie in ihrer schon früher geäußerten Kritik (vgl. ihre Entschließung vom 8./9. März 2007) bestätigt. Sie fordern den Gesetzgeber auf, die gesetzliche Regelung unter folgenden Aspekten nun zügig nachzubessern:

– Die Straftatenschwelle für Verkehrsdatenabfragen sollte insbesondere im Hinblick auf die inzwischen eingeführte Vorratsdatenspeicherung auf schwere Straftaten angehoben werden. Ein bedeutsamer Anteil der überprüften Verfahren war allenfalls der mittleren Kriminalität zuzuordnen.

– Die gesetzliche Höchstdauer der Maßnahme sollte von drei auf zwei Monate reduziert werden. Das Gutachten hat gezeigt, dass die praktischen Bedürfnisse, wie sie sich in den Aktendaten und Befragungsergebnissen äußern, dadurch vollständig abgedeckt würden.

– Für die Verkehrsdatenabfrage sollten (nach dem Vorbild der Regelungen für die akustische Wohnraumüberwachung) qualifizierte Begründungspflichten in der StPO vorgesehen werden. Dabei sollten auch die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen gesetzlich geregelt werden (z. B. Beweisverwertungsverbote). Wesentliche Kritikpunkte der Studie waren insbesondere die lediglich formelhafte Wiedergabe des Gesetzestextes sowie die häufig wörtliche Übernahme der staatsanwaltschaftlichen Anträge in den Begründungen.

– Zur Vermeidung von Rechtsunsicherheit und zur Stärkung des Richtervorbehalts sollte in den Fällen staatsanwaltschaftlicher Eilanordnung die Verwertbarkeit der erlangten Daten davon abhängig gemacht werden, dass ein Gericht rückwirkend die formelle und materielle Rechtmäßigkeit der Maßnahme feststellt. Dem Gutachten zufolge besteht insbesondere bei den Telekommunikationsunternehmen Unsicherheit, inwieweit sie zur Herausgabe der Verkehrsdaten verpflichtet sind, wenn eine staatsanwaltschaftliche Eilanordnung nicht innerhalb der gesetzlichen Frist richterlich bestätigt wird.

– Der tatsächliche Nutzen der Vorratsdatenspeicherung für die Strafverfolgung und damit die Erforderlichkeit der Maßnahme müssen in Frage gestellt werden. Bereits bei der früheren Höchstspeicherdauer von 3 Monaten waren nach der Studie 98 % der Abfragen erfolgreich.

Auch in der praktischen Anwendung der Regelungen zur Verkehrsdatenabfrage hat die Studie Defizite deutlich gemacht. Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher auch an die Strafverfolgungsbehörden und Gerichte, aus dem Gutachten Konsequenzen zu ziehen. Besonderes Augenmerk ist vor allem auf die Prüfung der Angemessenheit der Maßnahme zu richten. Dies muss auch in substantiierten Begründungen zum Ausdruck kommen. Die gesetzlich festgeschriebenen, dem Grundrechtsschutz dienenden Benachrichtigungs-, Löschungs- und Dokumentationspflichten müssen trotz hoher Belastungen in der Praxis unbedingt eingehalten werden. Der Richtervorbehalt muss seine grundrechtssichernde Funktion effizient erfüllen können. Die Justizverwaltungen sind in der Verantwortung, hierfür ausreichende personelle Ressourcen zur Verfügung zu stellen.

Eine Fortführung der wissenschaftlichen Evaluation der Verkehrsdatenabfrage ist unter den neuen rechtlichen Rahmenbedingungen und aufgrund der Weiterentwicklung der Technik unerlässlich. Insbesondere sollten dabei Notwendigkeit

und Nutzen der Verkehrsdatenabfrage auch im Vergleich zu anderen möglichen Maßnahmen mit Blick auf den Verhältnismäßigkeitsgrundsatz auf den Prüfstand gestellt werden.

Adress- und Datenhandel nur mit Einwilligung der Betroffenen

Der auf dem „Datenschutzgipfel“ im September 2008 gefundene Konsens, den Adress- und Datenhandel zukünftig nur auf der Grundlage einer Einwilligung zuzulassen, ist in Politik und Gesellschaft auf breite Zustimmung gestoßen. Nur eine solche Lösung respektiert das informationelle Selbstbestimmungsrecht und damit die Wahlfreiheit der Verbraucherinnen und Verbraucher. Wer davon jetzt abrücken will, verkennt die auf Grund der jüngsten Datenskandale ans Licht gekommenen Missstände, deren Ursache nicht nur in der kriminellen Energie Einzelner zu suchen ist. Um die Daten der Betroffenen tatsächlich wirksam schützen zu können, muss die Wahlmöglichkeit der Menschen von Maßnahmen flankiert werden, die die Herkunft der Daten jederzeit nachvollziehbar machten.

Die von der Werbewirtschaft gegen die Einwilligungslösung ins Feld geführten Argumente sind nicht überzeugend. Die behaupteten negativen Folgen für den Wirtschaftsstandort sind nicht zu belegen. Unabhängig davon gilt: Es gibt keine schutzwürdigen Interessen für die Beibehaltung von Geschäftsmodellen, die darauf beruhen, hinter dem Rücken und ohne Information der Betroffenen mit deren Daten Handel zu treiben. Die Einführung des Einwilligungsprinzips würde im Gegenteil zielgenaueres und wirksameres Direktmarketing erlauben. Die Bundesregierung sollte sich deshalb nicht von ihrer Absicht abbringen lassen, die beim „Datenschutzgipfel“ gegebenen Zusagen zur schnellen Verbesserung des Datenschutzes einzulösen. Sie würde es sonst versäumen, die notwendigen Lehren aus den jüngsten Skandalen zu ziehen. Der Referentenentwurf des Bundesinnenministeriums zur Änderung des Bundesdatenschutzgesetzes im Bereich des Adress- und Datenhandels (Stand: 22.10.2008) zieht mit der Einwilligungslösung – bei aller Verbesserungswürdigkeit im Detail – die einzig richtige und notwendige Konsequenz aus den zahlreichen Datenskandalen und darf nicht verwässert werden.

Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten

Mit der Gesundheitsreform soll über die Einführung von Wettbewerbsmechanismen die Qualität und Effizienz der gesetzlichen Krankenkassen verbessert wer-

den. Die Kassen sind daher bemüht und auch vom Gesetzgeber gehalten, Versicherten ein Versorgungsmanagement anzubieten. Von zentraler Bedeutung sind dabei Patientenschulungsmaßnahmen und strukturierte Behandlungsprogramme für chronisch kranke Versicherte, die jedoch lediglich Angebotscharakter haben dürfen. Ihre Teilnahme soll nach dem Willen des Gesetzgebers freiwillig sein und eine eingehende Unterrichtung voraussetzen. Diese Vorgaben werden von einzelnen Krankenkassen nicht beachtet, wenn sie versuchen, die Versicherten in ihrem Gesundheitsverhalten zu steuern und sie in bestimmte Maßnahmen und Programme zu drängen. Um Teilnehmerinnen und Teilnehmer zu gewinnen und um Maßnahmen durchzuführen, bedienen sich die Kassen vielfach privater Dienstleister und offenbaren diesen teils höchst sensible Gesundheitsdaten ihrer Versicherten. Dies ist datenschutzrechtlich nach dem Sozialgesetzbuch unzulässig, wenn die Übermittlung ohne Kenntnis und vorherige Einwilligung der jeweiligen Versicherten erfolgt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält die Einhaltung insbesondere der folgenden Eckpunkte bei gesundheitlichen Steuerungsprogrammen der Krankenkassen für unerlässlich:

- Die Krankenkassen dürfen Versichertendaten nur dann zur Auswahl von Personen für besondere Gesundheitsmaßnahmen verwenden, wenn dies gesetzlich ausdrücklich vorgesehen ist. Es muss sich um valide und erforderliche Daten handeln. Mit der Auswahl darf kein privater Dienstleister beauftragt werden.

- Die erstmalige Kontaktaufnahme mit potenziell für eine Gesundheitsmaßnahme in Betracht kommenden Versicherten muss durch die Krankenkasse selbst erfolgen, auch wenn ein privater Dienstleister mit der späteren Durchführung der Gesundheitsmaßnahme beauftragt worden ist.

- Die Versicherten sind vor Übermittlung ihrer Daten umfassend zu informieren. Die Information muss auch den Umstand umfassen, dass ein privates Unternehmen mit der Durchführung betraut werden soll. Soweit die Versicherten ausdrücklich in die Teilnahme eingewilligt haben, dürfen die für die Durchführung der Maßnahme erforderlichen Daten an den Dienstleister übermittelt werden.

- Wenn Versicherte zu welchem Zeitpunkt auch immer eindeutig zum Ausdruck bringen, nicht an einer Maßnahme teilnehmen zu wollen oder nicht an weitergehenden Informationen, einer konkreten Anwerbung oder einer fortgesetzten Betreuung interessiert zu sein, ist dies zu respektieren. Weitere Maßnahmen (auch telefonische Überredungsversuche) sind zu unterlassen.

Elektronische Steuererklärung sicher und datenschutzgerecht gestalten

Mit dem Steuerbürokratieabbaugesetz (BR-Drs. 547/08) sollen u. a. verfahrenstechnische Regelungen für die elektronische Übermittlung von Steuererklärungen durch Steuerpflichtige festgelegt werden. Zu diesem Zweck soll § 150 Abgabenordnung (AO) durch Abs. 7 Satz 1 dahingehend ergänzt werden, dass bei Einführung einer Verpflichtung zur elektronischen Abgabe die übermittelten Steuerdaten mit einer qualifizierten Signatur nach dem Signaturgesetz zu versehen sind.

Die Konferenz sieht es kritisch, dass § 150 Abs. 7 Satz 2 Nr. 6 und 7 AO auch vorsieht, zur Erleichterung und Vereinfachung des automatisierten Besteuerungsverfahrens anstelle der qualifizierten elektronischen Signatur ein so genanntes anderes sicheres Verfahren im Benehmen mit dem Bundesinnenministerium zuzulassen oder sogar auf beide Verfahren vollständig zu verzichten. In der Gesetzesbegründung wird darauf verwiesen, dass neben der qualifizierten elektronischen Signatur künftig auch eine Übermittlung der Daten unter Nutzung der Möglichkeiten des neuen elektronischen Personalausweises möglich sein soll.

Bereits in ihrer Entschließung zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren vom 11. Oktober 2006 hat die Konferenz gefordert, Nutzenden die Möglichkeit zu eröffnen, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt daher die vorgesehene Regelung in der AO zur Nutzung der qualifizierten elektronischen Signatur, da dieses Verfahren geeignet ist, die Authentizität und Integrität eines elektronisch übermittelten Dokuments sicherzustellen, und somit die handschriftliche Unterschrift ersetzen kann.

Die Datenschutzbeauftragten des Bundes und der Länder erklären hierzu:

1) Das Verfahren der qualifizierten elektronischen Signatur nach dem Signaturgesetz ist im Hinblick auf die Authentizität und Integrität elektronisch übermittelter Dokumente derzeit alternativlos.

2) Für die Bewertung anderer Verfahren sollte unmittelbar auf die Fachkenntnis unabhängiger Gutachter abgestellt werden. Als Gutachter für die Beurteilung der technischen Sicherheit kämen etwa die Bundesnetzagentur oder das BSI in Frage.

3) Steuerpflichtige müssen auch im elektronischen Besteuerungsverfahren die Möglichkeit haben, die elektronische Kommunikation mit der Finanzverwaltung durch das hierfür geeignete Verfahren der qualifizierten elektronischen Signatur abzusichern.

Gegen Blankettbefugnisse für die Software-Industrie

Gegenwärtig wird auf europäischer Ebene über Änderungen der Richtlinie zum Datenschutz in der elektronischen Kommunikation (2002/58/EG) beraten. Dabei geht es auch um die Frage, ob in Zukunft einzelfallunabhängig Verkehrsdaten zur Gewährleistung der Netz- und Informationssicherheit, also etwa zur Verfolgung von Hackerangriffen, verarbeitet werden dürfen.

Bereits auf der Grundlage der geltenden Richtlinie erlaubt § 100 Telekommunikationsgesetz den Telekommunikationsdiensteanbietern eine zielgerichtete, einzelfallbezogene Datenverarbeitung zur Fehlerbeseitigung und Missbrauchsbekämpfung. Diese Regelung hat sich in der Praxis bewährt. Es ist daher nicht erforderlich, zur Gewährleistung der Netz und Informationssicherheit einzelfallunabhängig personenbezogene Verkehrsdaten zu speichern. Die Anbieter von Telekommunikationsdiensten sind aufgefordert, ihre Systeme so sicher zu gestalten, dass Angriffe von vornherein erfolglos bleiben.

Obwohl die Europäische Kommission eine Änderung der bisherigen Rechtslage nicht für erforderlich hält, schlagen mehrere Mitgliedstaaten bei den gegenwärtigen Beratungen im Rat vor, entsprechend den Vorstellungen der Software-Industrie (Business Software Alliance) eine generelle Ermächtigung in die Richtlinie aufzunehmen, wonach *„jede natürliche oder juristische Person mit einem berechtigten Interesse“* berechtigt sein soll, Verkehrsdaten zu verarbeiten, um „technische Maßnahmen zur Gewährleistung der Sicherheit eines öffentlichen Telekommunikationsdienstes, eines öffentlichen oder privaten Telekommunikationsnetzes, eines Dienstes der Informationsgesellschaft oder von Endgeräten zu deren Nutzung“ zu ergreifen. Damit wäre nicht nur der jeweilige Diensteanbieter, der Maßnahmen zum Schutz des eigenen Angebots treffen will, zur einzelfallunabhängigen Speicherung von Verkehrsdaten berechtigt, sondern praktisch jeder mit einem wirtschaftlichen Verarbeitungsinteresse, insbesondere auch die Hersteller von Sicherheitssoftware.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt eine solche zeitlich unbegrenzte und inhaltlich unbestimmte Blankett-Ermächtigung als inakzeptabel ab. Der Hinweis auf die „Informationssicherheit“ rechtfertigt es nicht, dass Verkehrsdaten nahezu uferlos auch von Dritten verarbeitet werden. Die Bundesregierung wird aufgefordert, einer derartigen Aufweichung des Telekommunikationsgeheimnisses im Rat ihre Zustimmung zu verweigern.

II. Düsseldorfer Kreis – Oberste Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich

1. Beschlüsse der Sitzung am 17./18. April 2008 in Wiesbaden

Datenschutzkonforme Gestaltung sozialer Netzwerke

Der datenschutzgerechten Gestaltung sozialer Netzwerke im Internet kommt eine zentrale Bedeutung zu. Die Aufsichtsbehörden rufen in diesem Zusammenhang in Erinnerung, dass Anbieter in Deutschland zur Einhaltung des Regulierungsrahmens zum Datenschutz verpflichtet sind.

Insbesondere sind folgende rechtliche Rahmenbedingungen einzuhalten:

– Anbieter sozialer Netzwerke müssen ihre Nutzer umfassend gemäß den gesetzlichen Vorschriften über die Verarbeitung ihrer personenbezogenen Daten und ihre Wahl- und Gestaltungsmöglichkeiten unterrichten. Das betrifft auch Risiken für die Privatsphäre, die mit der Veröffentlichung von Daten in Nutzerprofilen verbunden sind. Darüber hinaus haben die Anbieter ihre Nutzer aufzuklären, wie diese mit personenbezogenen Daten Dritter zu verfahren haben.

– Die Aufsichtsbehörden weisen darauf hin, dass nach den Bestimmungen des Telemediengesetzes (TMG) eine Verwendung von personenbezogenen Nutzungsdaten für Werbezwecke nur zulässig ist, soweit die Betroffenen wirksam darin eingewilligt haben. Bei Werbemaßnahmen aufgrund von Profildaten müssen die Betroffenen nach den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) mindestens eine Widerspruchsmöglichkeit haben. Die Aufsichtsbehörden empfehlen, dass die Anbieter die Nutzer selbst darüber entscheiden lassen, ob – und wenn ja, welche – Profil- oder Nutzungsdaten zur zielgerichteten Werbung durch den Anbieter genutzt werden.

– Die Aufsichtsbehörden erinnern weiterhin daran, dass eine Speicherung von personenbezogenen Nutzungsdaten über das Ende der Verbindung hinaus ohne Einwilligung der Nutzer nur gestattet ist, soweit die Daten zu Abrechnungszwecken gegenüber dem Nutzer erforderlich sind.

– Für eine vorauseilende Speicherung von Daten über die Nutzung sozialer Netzwerke (wie auch anderer Internet-Dienste) für eventuelle zukünftige Strafverfolgung besteht keine Rechtsgrundlage. Sie wird insbesondere auch nicht durch die Regelungen zur Vorratsdatenspeicherung vorgeschrieben.

– Schließlich weisen die Aufsichtsbehörden darauf hin, dass das TMG die Anbieter dazu verpflichtet, das Handeln in sozialen Netzwerken anonym oder unter Pseudonym zu ermöglichen. Dies gilt unabhängig von der Frage, ob ein Nutzer sich gegenüber dem Anbieter des sozialen Netzwerks mit seinen Echtdaten identifizieren muss.

– Die Anbieter sind verpflichtet, die erforderlichen technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Sie müssen insbesondere einen systematischen oder massenhaften Export oder Download von Profildaten aus dem sozialen Netzwerk verhindern.

– Bei der datenschutzfreundlichen Gestaltung von sozialen Netzwerken kommt den Standardeinstellungen – z. B. für die Verfügbarkeit von Profildaten für Dritte – eine zentrale Bedeutung zu. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch die die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Kinder richtet. Der Zugriff durch Suchmaschinen darf jedenfalls nur vorgesehen werden, soweit der Nutzer ausdrücklich eingewilligt hat.

– Der Nutzer muss die Möglichkeit erhalten, sein Profil auf einfache Weise selbst zu löschen. Schließlich sollten die Anbieter sozialer Netzwerkdienste die Einführung von Verfallsdaten oder zumindest automatische Sperrungen erwägen, die von den Nutzern selbst festgelegt werden können.

Internet-Portale zur Bewertung von Einzelpersonen

1. Die Datenschutzaufsichtsbehörden weisen darauf hin, dass es sich bei Beurteilungen und Bewertungen von Lehrerinnen und Lehrern sowie von vergleichbaren Einzelpersonen in Internet-Portalen vielfach um sensible Informationen und subjektive Werturteile über Betroffene handelt, die in das Portal eingestellt werden, ohne dass die Urheber erkennbar sind und die jederzeit von jedermann abgerufen werden können.

2. Anbieter entsprechender Portale haben die Vorschriften des Bundesdatenschutzgesetzes über die geschäftsmäßige Verarbeitung personenbezogener Daten einzuhalten.

3. Bei der danach gesetzlich vorgeschriebenen Abwägung ist den schutzwürdigen Interessen der bewerteten Personen Rechnung zu tragen. Das Recht auf freie Meinungsäußerung rechtfertigt es nicht, das Recht der Bewerteten auf informationelle Selbstbestimmung generell als nachrangig einzustufen.

Keine fortlaufenden Bonitätsauskünfte an den Versandhandel

Auskunfteien dürfen Bonitätsauskünfte gemäß § 29 Absatz 2 Nr. 1a BDSG grundsätzlich nur erteilen, wenn der Dritte, dem die Daten übermittelt werden sollen, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat. Besteht zwischen diesem Dritten (also dem anfragenden Unternehmen) und dem Betroffenen ein Dauerschuldverhältnis, aufgrund dessen das anfragende Unternehmen während der gesamten Dauer des Bestehens ein finanzielles Ausfallrisiko trägt (z. B. Ratenzahlungskredit, Girokonto, Energielieferungs-, Telekommunikationsvertrag), so dürfen Bonitätsauskünfte nicht nur zu dem Zeitpunkt erteilt werden, zu dem der Betroffene ein solches Vertragsverhältnis beantragt hat, sondern während der gesamten Laufzeit des Vertragsverhältnisses und bis zur Erfüllung sämtlicher Pflichten des Betroffenen.

Ein Versandhandelsgeschäft stellt als solches kein Dauerschuldverhältnis dar. Die aufgrund der bisherigen Erfahrungen mit den Kunden möglicherweise bestehende Wahrscheinlichkeit und darauf gegründete Erwartung, dass der Kunde nach der ersten Bestellung wiederholt bestellen wird, und die zur Erleichterung der Bestellvorgänge möglicherweise erfolgte Einrichtung eines „Kundenkontos“ rechtfertigten es nicht, ein Versandhandelsgeschäft mit einem Dauerschuldverhältnis gleichzusetzen.

Ein berechtigtes Interesse seitens des Versandhandels gem. § 29 BDSG ist demnach nur gegeben, wenn aufgrund eines konkreten Bestellvorgangs ein finanzielles Ausfallrisiko vorliegt.

Nach Vertragsschluss sind Bonitätsauskünfte an Versandhändler dann nicht zu beanstanden, wenn ein Ratenzahlungskredit vereinbart wurde oder noch ein offener Saldo besteht. In allen anderen Fällen ist das Rechtsgeschäft nach Abwicklung des einzelnen Kaufgeschäftes für den Versandhandel abgeschlossen, ein berechtigtes Interesse an Bonitätsauskünften ist dann nicht mehr zu belegen. Damit sind Nachmeldungen oder sonstige Beauskunftungen in dieser Konstellation rechtlich unzulässig.

Hinweis:

Die Vertreter des Versandhandels und der Auskunfteien haben sich bereit erklärt, ihre Verfahren entsprechend den vorgenannten gesetzlichen Anforderungen bis spätestens Ende September 2008 umzustellen.

2. Beschlüsse der Sitzung am 13./14. November 2008 in Wiesbaden

Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet

Bei digital erfassten Fotos von Gebäude- und Grundstücksansichten, die über Geokoordinaten eindeutig lokalisiert und damit einer Gebäudeadresse und dem Gebäudeeigentümer sowie den Bewohnern zugeordnet werden können, handelt es sich in der Regel um personenbezogene Daten, deren Erhebung und Verarbeitung nach dem Bundesdatenschutzgesetz zu beurteilen ist. Die Erhebung, Speicherung und Bereitstellung zum Abruf ist nur zulässig, wenn nicht schutzwürdige Interessen der Betroffenen überwiegen. Bei der Beurteilung schutzwürdiger Interessen ist von Bedeutung, für welche Zwecke die Bilddaten verwendet werden können und an wen diese übermittelt bzw. wie diese veröffentlicht werden. Die obersten Aufsichtsbehörden sind sich einig, dass die Veröffentlichung von georeferenziert und systematisch bereit gestellten Bilddaten unzulässig ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind. Den betroffenen Bewohnern und Grundstückeigentümern ist zudem die Möglichkeit einzuräumen, der Veröffentlichung der sie betreffenden Bilder zu widersprechen und dadurch die Bereitstellung der Klarbilder zu unterbinden. Keine schutzwürdigen Interessen bestehen, wenn die Darstellung der Gebäude und Grundstücke so verschleiert bzw. abstrakt erfolgt, dass keine individuellen Eigenschaften mehr erkennbar sind. Um die Möglichkeit zum Widerspruch schon vor der Erhebung zu eröffnen, sollte die geplante Datenerhebung mit einem Hinweis auf die Widerspruchsmöglichkeit rechtzeitig vorher bekannt gegeben werden. Die Widerspruchsmöglichkeit muss selbstverständlich auch noch nach der Veröffentlichung bestehen.

Novellierung des Bundesdatenschutzgesetzes in den Bereichen Adressenhandel, Werbung und Datenschutzaudit

Der Düsseldorfer Kreis begrüßt, dass die Bundesregierung durch eine Novellierung des Bundesdatenschutzgesetzes aus den jüngst bekannt gewordenen Datenschutzverstößen im Bereich der Privatwirtschaft Konsequenzen ziehen möchte. Die uneingeschränkte Streichung des Listenprivilegs und die Pflicht zur Einholung einer Einwilligung des Betroffenen bei der Übermittlung an Dritte oder bei der Nutzung für Werbezwecke für Dritte sind erforderlich, um das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger zu stärken. Hiervon wird künftig auch die Wirtschaft profitieren. Die geplanten Änderungen ermöglichen es, Werbung zielgerichteter und ohne Streuverluste vorzunehmen und unerwünschte Belästigungen zu vermeiden, so dass das Verbrauchervertrauen in die Datenverarbeitung der Wirtschaft gestärkt wird. Die vorgesehenen Regelungen

zur Klarstellung, wann eine wirksame Einwilligung in die Werbenutzung vorliegt, und dass diese nicht mit wichtigen vertraglichen Gegenleistungen gekoppelt werden darf, verbessern die Transparenz und die Freiwilligkeit für den Betroffenen.

Darüberhinaus hat die beim Datenschutzgipfel am 4. September 2008 eingesetzte Länderarbeitsgruppe weitere Vorschläge zur Verbesserung des Bundesdatenschutzgesetzes unterbreitet, die jedoch bisher nicht berücksichtigt wurden.

Die derzeit geplanten Vorschriften genügen nicht, um künftig im Bereich der privaten Wirtschaft ein ausreichendes Datenschutzniveau zu verwirklichen. Hierzu bedarf es zum einen einer angemessenen Ausstattung der Datenschutzaufsichtsbehörden. Es bedarf zum anderen gemäß den europarechtlichen Vorgaben wirksamer Einwirkungsbefugnisse. Hierzu gehört neben adäquaten Kontroll- und Sanktionsmitteln die Möglichkeit, bei schwerwiegenden Datenschutzverstößen die Erhebung und Verwendung personenbezogener Daten zu untersagen. Auch die Stellung der betrieblichen Datenschutzbeauftragten sollte gestärkt werden.

Die bisherigen Vorschläge des Bundesministeriums des Innern zur Einführung eines Datenschutzaudits sind nicht geeignet, den Datenschutz in der Wirtschaft zu verbessern.

III. Europäische Konferenz der Datenschutzbeauftragten

Rom, 17./18. April 2008

Erklärung

Die Europäische Union wird in Kürze über verschiedene neue Initiativen zur verbesserten Kontrolle von Reisenden in die Europäische Union und aus der Europäischen Union, diskutieren. Drei von der Kommission vor kurzem verabschiedete Mitteilungen[1] haben zum Ziel, eine solche Diskussion über die nächsten Schritte zum Border Management, sowie über die Schaffung eines Europäischen Grenzüberwachungssystems und über die Bewertung von Frontex in Gang zu bringen.

Zusammen mit den Maßnahmen, die bereits eingeführt wurden oder bald eingeführt werden sollen, und die auf eine verbesserte Überwachung von Reisenden für Grenzkontrollen, Visum-Politik und Strafverfolgungsmaßnahmen abzielen, lassen die aktuellen Mitteilungen deutlich eine Entwicklung in Richtung einer vollständigen Kontrolle und Überwachung von Personen– unabhängig von ihrer Nationalität – die in das Schengen-Gebiet einreisen oder ausreisen, erkennen.

Obwohl ein effizientes Border Management für den Schutz der Union gegen mögliche Bedrohungen notwendig ist, so darf dies niemals in unverhältnismäßiger Weise die Rechte und Freiheiten der Reisenden, und vor allem nicht deren Recht auf Privatsphäre verletzen. Die Überwachung der Reisenden muss wohlbegründet sein und darf nur in Ausnahmefällen gestattet werden, und dies auch nur für berechtigte und besondere Zwecke. Jede allgemeine Überwachung stellt nicht hinnehmbare Risiken für die Freiheit der Einzelnen dar.

Ein anderes Thema, das überdacht werden muss, ist das zu Grunde liegende Konzept, Reisenden zu misstrauen, in dem man ausgewählte „vertrauenswürdige“ Reisende von allen anderen Reisenden isoliert, und die letzteren sogar als potentielle Straftäter erachtet. Das wird eine Durchleuchtung vor und am Eingang beinhalten, so wie die Kontrolle der Grenzüberschreitungen und die automatische Verarbeitung spezieller Daten der Reisenden. Dieses Konzept trägt nicht gerade viel dazu bei, den „symbolischen Effekt, die EU als weltoffen darzustellen“[2], zu

[1] KOM (2008) 69 endg.
KOM (2008) 68 endg.
KOM (2008) 67 endg.

[2] KOM (2008) 69 endg. Seite 6.

verwirklichen, so wie es die Mitteilung der Kommission erwähnt, und es ist sogar fraglich, ob dies mit den Werten der Europäischen Union im Einklang steht.

Die Konferenz hat bereits die Mitglieder der Europäischen Union und die Kommission, den Rat und das Europäische Parlament dazu aufgerufen, zuerst einmal eine Evaluierung zu fertigen, ob die bereits bestehenden rechtlichen Maßnahmen effektiv umgesetzt und durchgeführt werden.[3] Ein neuer Vorschlag sollte nur dann eingebracht werden und wenn klare Hinweise vorliegen, die solche Maßnahmen unterstützen.

Allerdings fand bis jetzt keine solche Bewertung über die Effektivität der Umsetzung der bestehenden rechtlichen Maßnahmen statt. Auch wurden keine verlässlichen Hinweise vorgelegt, die die Notwendigkeit neuer Systeme untermauern. Ebenso wenig wurden Beweise erbracht, die es erforderlich erscheinen lassen, die aktuellen Initiativen auf diesem Gebiet zu ergänzen.

Die von der Kommission vorgelegten Informationen über die geplanten Systeme liefern keinen klaren Beweis für ihre Effektivität. In Bezug auf die direkten und indirekten Kosten im Hinblick auf die Freiheiten und die Bürgerrechte – ganz abgesehen von den finanziellen Aspekten – für die Schaffung neuer Systeme wie zum Beispiel das Einreise-Ausreise-System, sollten auch aussagekräftige Beweise vorliegen, dass dieses System die beste Antwort auf das Problem ist, das es in Angriff nehmen soll.

Da dies anscheinend nicht der Fall ist, ruft die Konferenz die Europäische Union auf, die Notwendigkeit und Verhältnismäßigkeit weiterer Maßnahmen im Lichte der oben erwähnten Kommentare sorgfältig zu überdenken, und zwar vor allem in Bezug auf die in den Mitteilungen der Kommission vorgesehenen Vorschläge.

[3] Erklärung von Larnaka über die Verfügbarkeit, Mai 2007

IV. Dokumente der Europäischen Union: Artikel 29-Datenschutzgruppe

Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen (WP 148)

Angenommen am 4. April 2008

Inhaltsverzeichnis

ZUSAMMENFASSUNG

Suchmaschinen sind zu einem festen Bestandteil des Alltags der Menschen geworden, die das Internet und Technologien zur Informationsgewinnung nutzen. Die Artikel-29-Datenschutzgruppe ist sich der Nützlichkeit von Suchmaschinen bewusst und erkennt ihre Bedeutung an.

In der vorliegenden Stellungnahme benennt die Arbeitsgruppe klare Verantwortlichkeiten im Rahmen der Datenschutzrichtlinie (95/46/EG) für Suchmaschinenbetreiber in ihrer Rolle als Verantwortliche für die Verarbeitung von Benutzerdaten. In bestimmten Situationen ist das europäische Datenschutzrecht auch auf Suchmaschinen anwendbar, wenn sie als Anbieter von Inhaltsdaten (d. h. Index der Suchergebnisse) fungieren, z. B. wenn sie einen Caching-Dienst anbieten oder sich auf die Erstellung von Personenprofilen spezialisieren. Vorrangiges Ziel dieser Stellungnahme ist es, ein Gleichgewicht zwischen den berechtigten geschäftlichen Erfordernissen der Suchmaschinenbetreiber und dem Schutz der personenbezogenen Daten von Internet-Benutzern herzustellen.

Diese Stellungnahme befasst sich mit der Definition von Suchmaschinen, den Arten der bei der Bereitstellung von Suchdiensten verarbeiteten Daten, dem Rechtsrahmen, den Zwecken/Gründen für eine zulässige Verarbeitung, der Verpflichtung zur Information der betroffenen Personen und den Rechten der betroffenen Personen.

Eine wichtige Schlussfolgerung dieser Stellungnahme besteht darin, dass die Datenschutzrichtlinie grundsätzlich auf die Verarbeitung personenbezogener Daten durch Suchmaschinen anwendbar ist, auch wenn sich deren Hauptsitz außerhalb des EWR befindet, und dass es unter diesen Umständen Sache der Suchmaschinenbetreiber ist, ihre Rolle im EWR und den Umfang ihrer Verantwortlichkeiten im Rahmen der Richtlinie zu klären. Des Weiteren wird klargestellt, dass die Richtlinie über die Vorratsspeicherung von Daten (2006/24/EG) eindeutig nicht auf Suchmaschinenbetreiber anwendbar ist.

Die vorliegende Stellungnahme kommt zu dem Ergebnis, dass personenbezogene Daten nur für rechtmäßige Zwecke verarbeitet werden dürfen. Die Suchmaschinenbetreiber müssen personenbezogene Daten löschen oder irreversibel anonymisieren, sobald sie der angegebenen rechtmäßigen Zweckbestimmung nicht mehr dienen, und sie müssen in der Lage sein, die Speicherung und die Lebensdauer der gesetzten Cookies jederzeit zu begründen. Bei allen geplanten Querverbindungen von Benutzerdaten und bei der Anreicherung von Benutzerprofilen muss die Einwilligung des Benutzers eingeholt werden. Die Suchmaschinen müssen Nichtbeteiligungsklauseln („Opt-outs“) von Website-Herausgebern beachten und den Aufforderungen von Benutzern zur Aktualisierung oder Auffrischung ihrer Cache-Speicher unverzüglich nachkommen. Die Arbeitsgruppe er-

innert in diesem Zusammenhang an die Verpflichtung der Suchmaschinen, die Benutzer im Vorhinein über alle beabsichtigten Verwendungszwecke ihrer Daten zu informieren und ihre Rechte auf Auskunft, Einsichtnahme oder Berichtigung ihrer personenbezogenen Daten gemäß Artikel 12 der Datenschutzrichtlinie (95/46/EG) zu respektieren.

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 und auf Artikel 30 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie sowie Artikel 15 Absatz 3 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002,

gestützt auf Artikel 255 EG-Vertrag und auf die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission,

gestützt auf ihre Geschäftsordnung,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG

Die Suchmaschinenbetreiber im World Wide Web erfüllen als Vermittler eine überaus wichtige Rolle in der Informationsgesellschaft. Die Arbeitsgruppe erkennt die Notwendigkeit und die Nützlichkeit von Suchmaschinen an und ist sich ihres Beitrags zur Entwicklung der Informationsgesellschaft bewusst.

Für die unabhängigen Datenschutzbehörden im EWR spiegelt sich die wachsende Bedeutung der Suchmaschinen aus Datenschutzsicht in der steigenden Zahl der Beschwerden von Personen („betroffene Personen“) über mögliche Verstöße gegen ihr Recht auf Privatsphäre wider. Zudem ist die Zahl der Anfragen seitens der für die Verarbeitung Verantwortlichen sowie seitens der Presse bezüglich der Auswirkungen von Internet-Suchdiensten auf den Schutz personenbezogener Daten spürbar gestiegen.

[1] ABl. L 281 vom 23.11.1995, S. 31, http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

In den Beschwerden der betroffenen Personen spiegeln sich ebenso wie in den Anfragen der für die Verarbeitung Verantwortlichen und der Presse die zwei verschiedenen Rollen wider, die Suchmaschinenbetreiber in Bezug auf personenbezogene Daten spielen.

Erstens erheben und verarbeiten Suchmaschinenbetreiber in ihrer Rolle als Diensteanbieter gewaltige Mengen an Benutzerdaten, darunter auch Daten, die mit technischen Mitteln wie Cookies erfasst werden. Das Spektrum der erhobenen Daten kann von den IP-Adressen einzelner Benutzer bis hin zu umfangreichen Suchhistorien sowie Daten reichen, die bei der Anmeldung für die Nutzung personalisierter Dienste von den Benutzern selbst eingegeben wurden. Die Erhebung von Benutzerdaten wirft zahlreiche Fragen auf. Durch den Fall AOL wurde einem breiten Publikum die Sensibilität von personenbezogenen Daten, die in Suchprotokollen enthalten sind, deutlich vor Augen geführt.[2] Nach Auffassung der Arbeitsgruppe haben die Suchmaschinenbetreiber in ihrer Rolle als Sammler von Benutzerdaten die Benutzer ihrer Dienste bisher noch nicht ausreichend über die Art und den Zweck ihrer Tätigkeit informiert.

Zweitens tragen Suchmaschinenbetreiber in ihrer Rolle als Anbieter von Inhalten dazu bei, dass ein weltweites Publikum einfachen Zugriff auf Veröffentlichungen im Internet erhält. Einige Suchmaschinen veröffentlichen Daten in einem so genannten „Cache“ (Zwischenspeicher) erneut. Durch die Wiedergewinnung und Zusammenfassung verschiedener Arten von Informationen über eine einzelne Person können Suchmaschinen ein neues Bild entstehen lassen, das mit wesentlich höheren Risiken für die betroffene Person behaftet ist, als wenn jedes in das Internet eingestellte Datenelement für sich isoliert bleiben würde. Die Darstellungs- und Aggregierungsfunktionen von Suchmaschinen können weit reichende Folgen für die Menschen sowohl in ihrem Privatleben als auch in der Gesellschaft haben. Das gilt vor allem, wenn die personenbezogenen Daten in den Suchergebnissen unrichtig, unvollständig oder überzogen sind.

Am 15. April 1998 hat die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (International Working Group on Data Protection in Telecommunications – IWGDPT)[3] einen Gemeinsamen Standpunkt zu Datenschutz bei Suchmaschinen im Internet angenommen, der am 6./7. April 2006 überarbeitet wurde.[4] Die Arbeitsgruppe zeigte sich darin besorgt über die Möglichkeit von

---

2 Im Sommer 2006 veröffentlichte AOL eine Liste der Suchanfragen, die von rund 650 000 Benutzern über einen Zeitraum von drei Monaten in die AOL-Suchmaschine eingegeben worden waren. Obwohl AOL die Namen der Benutzer durch eine Zahl ersetzt hatte, fanden Journalisten heraus, dass die Ergebnisse der Suchanfragen oftmals zu den einzelnen Benutzern zurückverfolgt werden konnten, nicht nur wegen so genannter „Eitelkeitsanfragen“ (Suche mit eigenem Namen als Suchbegriff nach sich selbst), sondern auch aufgrund des Inhalts ihrer kombinierten Suchanfragen.

3 Die Arbeitsgruppe wurde auf Betreiben der Datenschutzbeauftragten verschiedener Länder gebildet, um die Privatsphäre und den Datenschutz in der Telekommunikation und in den Medien zu verbessern.

4 http://www.datenschutz-berlin.de/attachments/44/Dokumente1998.pdf?1164728350

Suchmaschinenbetreibern, Profile von natürlichen Personen erstellen zu lassen. In diesem Gemeinsamen Standpunkt wurde ausgeführt, wie bestimmte Aktivitäten von Suchmaschinenbetreibern die Privatsphäre der Bürger bedrohen können und dass personenbezogene Daten jeglicher Art, die auf einer Website eingestellt werden, von Dritten zur Erstellung von Personenprofilen verwendet werden könnten.

Außerdem wurde auf der 28. Internationalen Konferenz der Datenschutzbeauftragten am 2./3. November 2006 in London die Entschließung zum Datenschutz bei Suchmaschinen (Resolution on Privacy Protection and Search Engines)[5] angenommen. In der Entschließung werden die Betreiber von Suchmaschinen aufgefordert, die grundlegenden Regeln des Datenschutzes zu respektieren, wie sie in der nationalen Gesetzgebung vieler Länder sowie auch in internationalen Strategiepapieren und Verträgen niedergelegt sind, und gegebenenfalls ihre Praktiken entsprechend zu ändern. Darüber hinaus werden in der Entschließung verschiedene Aspekte im Zusammenhang mit Server-Protokollen, kombinierten Suchanfragen und deren Speicherung und der Erstellung detaillierter Profile von Benutzern erörtert.

2. DEFINITION FÜR „SUCHMASCHINE“ UND GESCHÄFTSMODELL

Generell sind unter Suchmaschinen Dienste zu verstehen, die ihren Benutzern beim Auffinden von Informationen im Internet helfen. Suchmaschinen können nach der Art der abzurufenden Daten unterschieden werden, darunter Bilder und/oder Videos und/oder Audiodaten oder verschiedene Arten von Formaten. Ein neues Entwicklungsgebiet sind Suchmaschinen, die sich auf die Erstellung von Personenprofilen auf Basis von personenbezogenen Daten spezialisiert haben, die irgendwo im Internet gefunden wurden.

Im Rahmen der Richtlinie über den elektronischen Geschäftsverkehr (2000/31/EG) werden Suchmaschinen als Dienste der Informationsgesellschaft[6] bezeichnet, d. h. als Instrumente zur Lokalisierung von Informationen[7]. Die Arbeitsgruppe verwendet diese Einstufung als Ausgangspunkt.

Die Arbeitsgruppe konzentriert sich in dieser Stellungnahme hauptsächlich auf Suchmaschinenbetreiber, die sich am vorherrschenden Geschäftsmodell für

---

5 http://www.privacyconference2006.co.uk/index.asp?PageID=3

6 Internet-Suchmaschinen werden in den europäischen Rechtsvorschriften über die Dienste der Informationsgesellschaft behandelt, die in Artikel 2 der Richtlinie 2000/31/EG näher bezeichnet werden. Dieser Artikel verweist auf die Richtlinie 98/34/EG, die den Begriff „Dienst“ bzw. „Dienstleistung der Informationsgesellschaft“ spezifiziert.

7 Siehe Artikel 21 Absatz 2 in Verbindung mit dem Erwägungsgrund 18 der Richtlinie über den elektronischen Geschäftsverkehr (2000/31/EG).

Suchmaschinen orientieren und sich durch Werbung finanzieren. In diese Kategorie fallen alle großen und bekannten Suchmaschinen, spezialisierte Suchmaschinen, die sich auf die Erstellung von Personenprofilen konzentrieren, sowie Meta-Suchmaschinen, die die Ergebnisse anderer Suchmaschinen präsentieren und eventuell neu zusammenfassen. Die Stellungnahme befasst sich nicht mit Suchfunktionen, die in Websites eingebettet sind und sich auf die Datensuche in der eigenen Domäne der Website beschränken.

Die Rentabilität derartiger Suchmaschinen hängt gewöhnlich von der Wirksamkeit der Werbung ab, die in Verbindung mit den Suchergebnissen angezeigt wird. Die Einnahmen werden überwiegend mit einem Pay-per-Click- (PPC) Verfahren erzielt. Bei diesem Geschäftsmodell berechnet die Suchmaschine dem Werbetreibenden einen bestimmten Betrag, sobald ein Benutzer auf einen gesponserten Link klickt. Die Untersuchung der Genauigkeit der Suchergebnisse und Werbeanzeigen konzentriert sich überwiegend auf die richtige Kontextualisierung. Damit die Suchmaschine die gewünschten Ergebnisse liefert und die Werbeanzeigen zur Optimierung der Einnahmen auch bei den richtigen Zielgruppen geschaltet werden, versuchen die Suchmaschinen möglichst viel über die Eigenschaften und den Kontext jeder einzelnen Suchanfrage herauszufinden.

3. UM WELCHE ARTEN VON DATEN GEHT ES?

Suchmaschinen verarbeiten eine große Vielfalt an Daten.[8] Eine Liste der verschiedenen Arten von Daten findet sich im Anhang.

Protokolldateien

Die bei der Nutzung des Suchmaschinendienstes für den Benutzer angelegten Protokolldateien sind – sofern keine Anonymisierung erfolgt – die wichtigsten personenbezogenen Daten, die von den Suchmaschinenbetreibern verarbeitet werden. Die für die Nutzung des Dienstes typischen Daten lassen sich verschiedenen Kategorien zuordnen: Protokolle der Anfragen (Inhalt der Suchanfragen, Datum und Uhrzeit, Quelle (IP-Adresse und Cookie), benutzerspezifische Einstellungen und Daten, die sich auf den Computer des Benutzers beziehen); Daten über die angebotenen Inhalte (Links und Werbeanzeigen aufgrund jeder Anfrage) sowie Daten über die anschließende Benutzernavigation (Klicks). Die Suchma-

[8] Die Artikel-29-Arbeitsgruppe hat unter anderem einen Fragebogen zur Datenschutzerklärung erstellt. Der Fragebogen wurde einer Reihe von Suchmaschinenbetreibern in den Mitgliedstaaten sowie verschiedenen Suchmaschinenbetreibern mit Sitz in den USA vorgelegt. Diese Stellungnahme beruht teilweise auf der Auswertung der Antworten auf diesen Fragebogen. Der Fragebogen ist in Anhang 2 dieser Stellungnahme beigefügt.

schinen können auch operative Daten verarbeiten, die sich auf Benutzerdaten beziehen, Daten über registrierte Benutzer und Daten von anderen Diensten und aus anderen Quellen wie elektronische Post, Desktop-Suche und Werbeanzeigen auf Websites Dritter.

IP-Adressen

Ein Suchmaschinenbetreiber kann verschiedene Anfragen und Suchsitzungen, die von einer einzigen IP-Adresse ausgehen, miteinander verknüpfen.[9] Daher können bei der Protokollierung der Suchvorgänge alle Suchvorgänge im Internet, die von einer bestimmten IP-Adresse ausgehen, verfolgt und korreliert werden. Die Identifizierung kann noch verbessert werden, wenn die IP-Adresse mit einem vom Suchmaschinenbetreiber übermittelten Cookie mit benutzerspezifischer Kennung korreliert wird, da sich dieses Cookie auch dann nicht ändert, wenn die IP-Adresse geändert wird.

Die IP-Adresse kann ebenfalls als Lokalisierungsinformation verwendet werden, auch wenn sie derzeit noch oftmals ungenau ist.

Web-Cookies

Benutzer-Cookies werden von der Suchmaschine übermittelt und auf dem Computer des Benutzers gespeichert. Der Inhalt der Cookies kann je nach Suchmaschinenbetreiber unterschiedlich sein. Die von Suchmaschinen gesetzten Cookies enthalten typischerweise Informationen über das Betriebssystem und den Browser des Benutzers sowie eine eindeutige Identifikationsnummer für jedes Benutzerkonto. Sie ermöglichen eine genauere Identifizierung des Benutzers als die IP-Adresse. Wenn beispielsweise mehrere Benutzer mit jeweils eigenem Konto denselben Computer benutzen, würde jeder Benutzer ein eigenes Cookie erhalten, der ihn als Benutzer des Computers eindeutig identifiziert. Wenn ein Computer eine dynamische und variable IP-Adresse besitzt und die Cookies am Ende einer Sitzung nicht gelöscht werden, kann mit einem derartigen Cookie der Benutzer von einer IP-Adresse zur nächsten verfolgt werden. Das Cookie kann auch zur Korrelation von Suchvorgängen verwendet werden, die von nomadischen Computern wie beispielsweise Laptops gestartet werden, da ein Benutzer an verschiedenen Orten dasselbe Cookie hätte. Wenn sich mehrere Computer einen Internet-Anschluss teilen (z. B. hinter einer Box oder einem Router mit Adressübersetzung der Absenderadresse (Network Address Translation – NAT), ermöglicht das Cookie die Identifizierung der einzelnen Benutzer an den verschiedenen Computern.

[9] Immer mehr Internet-Diensteanbieter vergeben feste IP-Adressen an einzelne Benutzer.

Die Suchmaschinenbetreiber benutzen Cookies (gewöhnlich dauerhafte Cookies) zur Verbesserung der Qualität ihrer Dienstleistungen, indem sie die Benutzereinstellungen speichern und typische Merkmale des Benutzers, etwa sein Suchverhalten, verfolgen. Die meisten Browser sind standardmäßig so konfiguriert, dass sie Cookies akzeptieren. Der Browser kann aber auch so eingestellt werden, dass er alle Cookies ablehnt, nur Sitzungs-Cookies akzeptiert oder anzeigt, wann ein Cookie übermittelt wird. Eventuell funktionieren manche Merkmale und Dienste jedoch nicht richtig, wenn Cookies grundsätzlich abgelehnt werden, und zudem lassen sich erweiterte Funktionsmerkmale zur Cookie-Verwaltung nicht immer einfach konfigurieren.

Flash-Cookies

Einige Suchmaschinenbetreiber installieren Flash-Cookies auf dem Computer des Benutzers. Gegenwärtig können Flash-Cookies nicht ohne weiteres, etwa mit Hilfe der Standardlöschfunktionen der Internet-Browser, gelöscht werden. Bisher wurden Flash-Cookies unter anderem als Sicherung für normale Web-Cookies verwendet, die von den Benutzern leicht gelöscht werden können, oder auch zur Speicherung umfassender Informationen über Suchvorgänge der Benutzer (z. B. alle Internet-Anfragen, die an eine Suchmaschine übermittelt wurden).

4. RECHTSRAHMEN

4.1. Verantwortliche für die Verarbeitung von Benutzerdaten

4.1.1. Das Grundrecht – Achtung der Privatsphäre

Im Hinblick auf die umfassende Erhebung und die Speicherung der Suchhistorien von Personen in direkt oder indirekt identifizierbarer Form kommt der Schutz personenbezogener Daten gemäß Artikel 8 der Charta der Grundrechte der Europäischen Union zum Tragen.

Die Suchhistorie einer Person gibt Aufschluss über die Interessen, Beziehungen und Absichten dieser Person. Diese Daten können nachfolgend sowohl für kommerzielle Zwecke als auch – aufgrund von Anfragen und Phishing-Operationen und/oder Data Mining – von Strafverfolgungsbehörden oder nationalen Sicherheitsdiensten verwendet werden.

In Erwägungsgrund 2 der Richtlinie 95/46/EG heißt es: „Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnorts der natürlichen Personen, deren Grundrechte

und -freiheiten und insbesondere deren Privatsphäre zu achten und zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der Menschen beizutragen."

Die Suchmaschinen spielen eine entscheidende Rolle als erster Kontaktpunkt für den freien Zugriff auf Informationen im Internet. Dieser freie Zugriff auf Informationen ist für die persönliche Meinungsbildung in unserer Demokratie überaus wichtig. Aus diesem Grund ist Artikel 11 der Charta der Grundrechte der Europäischen Union von besonderer Bedeutung, da er vorsieht, dass Informationen ohne behördliche Eingriffe als Teil der Meinungsäußerung und Informationsfreiheit zugänglich sein sollten.

4.1.2. Anwendbarkeit der Richtlinie 95/46/EG (Datenschutzrichtlinie)

Die Artikel-29-Arbeitsgruppe hat sich bereits in ihren früheren Arbeitspapieren zu den Datenschutzbestimmungen aufgrund der Protokollierung von IP-Adressen und der Verwendung von Cookies im Rahmen der Dienste der Informationsgesellschaft geäußert. Die vorliegende Stellungnahme enthält weitere Leitlinien für die Anwendung der Definitionen von „personenbezogenen Daten" und „für die Verarbeitung Verantwortlicher" durch Suchmaschinenbetreiber. Suchmaschinendienste können im Internet innerhalb der EU bzw. des EWR, von einem Standort außerhalb des Hoheitsgebiets der EU/EWR-Mitgliedstaaten oder von mehreren Standorten in der EU bzw. im EWR und im Ausland bereitgestellt werden. Daher werden die Bestimmungen von Artikel 4 ebenfalls erörtert. Artikel 4 der Datenschutzrichtlinie befasst sich mit der Anwendbarkeit des einzelstaatlichen Datenschutzrechts.

Personenbezogene Daten: IP-Adressen und Cookies

In ihrer Stellungnahme (WP 136) zum Begriff „personenbezogene Daten" hat die Arbeitsgruppe einige Klarstellungen in Bezug auf die Definition „personenbezogene Daten" vorgenommen.[10] Bei der Suchhistorie einer Person handelt es sich um personenbezogene Daten, wenn die Person, auf die sich die Daten beziehen, bestimmbar ist. Obwohl die IP-Adressen in den meisten Fällen von den Suchmaschinen nicht direkt bestimmbar sind, kann eine Identifizierung dennoch durch Dritte erfolgen. Internet-Diensteanbieter speichern IP-Adressdaten. Strafverfolgungs- und nationale Sicherheitsbehörden können Zugriff auf diese Daten erhalten, und in einigen Mitgliedstaaten haben auch bereits Privatparteien durch Zivilprozesse Zugriff darauf erhalten. In den meisten Fällen – einschließlich Fällen mit dynamischer IP-Adresszuordnung – sind also die notwendigen

[10] WP 136, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf

Daten zur Identifizierung des Benutzers bzw. der Benutzer der IP-Adresse vorhanden.

Die Arbeitsgruppe weist in ihrem Arbeitspapier Nr. 136 auf Folgendes hin: *„Wenn der Internet-Diensteanbieter also nicht mit absoluter Sicherheit erkennen kann, dass die Daten zu nicht bestimmbaren Benutzern gehören, muss er sicherheitshalber alle IP-Informationen wie personenbezogene Daten behandeln.“*

Cookies

Wenn ein Cookie eine eindeutige Benutzerkennung enthält, handelt es sich bei dieser Kennung eindeutig um personenbezogene Daten. Dauerhafte Cookies oder ähnliche Mittel mit einer eindeutigen Benutzerkennung ermöglichen die Verfolgung der Benutzer eines bestimmten Computers selbst bei Verwendung dynamischer IP-Adressen.[11] Die Verhaltensdaten, die durch den Einsatz dieser Mittel generiert werden, ermöglichen eine noch stärkere Fokussierung auf die persönlichen Merkmale der betreffenden Person. Dies entspricht der grundlegenden Logik des vorherrschenden Geschäftsmodells.

Für die Verarbeitung Verantwortlicher

Ein Suchmaschinenbetreiber, der Benutzerdaten einschließlich der IP-Adressen und/oder dauerhafter Cookies mit eindeutiger Kennung verarbeitet, fällt unter die Definition des für die Verarbeitung Verantwortlichen, da er über die Zwecke und Mittel der Verarbeitung entscheidet. Das multinational ausgerichtete Geschäftsmodell der großen Suchmaschinenbetreiber – oftmals mit Hauptsitzen außerhalb des EWR, weltweiten Dienstleistungsangeboten, Beteiligung verschiedener Zweigstellen und eventuell auch Dritter an der Verarbeitung personenbezogener Daten – hat die Frage aufgeworfen, wer bei einer Verarbeitung von personenbezogenen Daten als der für die Verarbeitung Verantwortliche anzusehen ist.

Die Arbeitsgruppe möchte an dieser Stelle den Unterschied zwischen den Definitionen des Datenschutzrechts im EWR und der Frage betonen, ob das Datenschutzrecht in einer bestimmten Situation anwendbar ist. Ein Suchmaschinenbetreiber, der personenbezogene Daten wie z. B. Protokolle mit personenbezogenen Suchhistorien verarbeitet, ist für diese personenbezogenen Daten der für die Verarbeitung Verantwortliche unabhängig von der Frage nach der hoheitsrechtlichen Zuständigkeit.

[11] WP 136: „An diesem Punkt ist anzumerken, dass Personen in der Praxis zwar überwiegend anhand ihres Namens identifiziert werden, ein Name zur Identifizierung einer Person jedoch keineswegs immer notwendig ist. Beispielsweise kann eine Person anhand anderer „Kennzeichen“ singularisiert werden. So ordnen rechnergestützte Dateien zur Erfassung personenbezogener Daten den erfassten Personen gewöhnlich ein eindeutiges Kennzeichen zu, um Verwechslungen zwischen zwei Personen in der Datei auszuschließen.“

Artikel 4 der Datenschutzrichtlinie / Anwendbares einzelstaatliches Recht

Artikel 4 der Datenschutzrichtlinie befasst sich mit der Frage nach dem anwendbaren einzelstaatlichen Recht. In ihrem „Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU“[12] hat die Arbeitsgruppe weitere Leitlinien in Bezug auf die Bestimmungen von Artikel 4 formuliert. Hinter dieser Bestimmung stehen zwei Erwägungsgründe. Erstens geht es darum, Lücken im bestehenden System des gemeinschaftlichen Datenschutzes zu schließen und eine Umgehung dieses Systems zu vermeiden. Zweitens geht es darum, die Möglichkeit auszuschließen, dass ein und derselbe Verarbeitungsvorgang den Rechtsvorschriften von mehr als einem EU-Mitgliedstaat unterliegt. Aufgrund des multinationalen Charakters der von den Suchmaschinen ausgelösten Datenströme befasst sich die Arbeitsgruppe mit beiden Sachverhalten.

Bei der Verarbeitung personenbezogener Daten durch einen Suchmaschinenbetreiber, der in einem oder in mehreren Mitgliedstaaten niedergelassen ist und all seine Dienstleistungen dort erbringt, fällt die Verarbeitung personenbezogener Daten eindeutig in den Anwendungsbereich der Datenschutzrichtlinie. In diesem Fall ist es wichtig zu beachten, dass die Datenschutzbestimmungen nicht auf die betroffenen Personen im Hoheitsgebiet oder mit einer Staatsangehörigkeit eines der Mitgliedstaaten beschränkt sind.

Ist der Suchmaschinenbetreiber ein nicht im EWR ansässiger für die Verarbeitung Verantwortlicher, so ist das gemeinschaftliche Datenschutzrecht in zwei Fällen dennoch anwendbar, und zwar erstens, wenn der Suchmaschinenbetreiber eine Niederlassung in einem Mitgliedstaat im Sinne von Artikel 4 Absatz 1 Buchstabe a besitzt, und zweitens, wenn die Suchmaschine auf Mittel im Hoheitsgebiet eines Mitgliedstaats im Sinne von Artikel 4 Absatz 1 Buchstabe c zurückgreift. Im zweiten Fall muss der Suchmaschinenbetreiber gemäß Artikel 4 Absatz 2 einen im Hoheitsgebiet des genannten Mitgliedstaats ansässigen Vertreter benennen.

Niederlassung im Hoheitsgebiet eines Mitgliedstaats (EWR)

Gemäß Artikel 4 Absatz 1 Buchstabe a ist das Datenschutzrecht eines Mitgliedstaats anzuwenden, wenn bei der Verarbeitung personenbezogener Daten bestimmte Vorgänge durch den für die Verarbeitung Verantwortlichen „im Rahmen der Tätigkeiten einer Niederlassung“ ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet eines Mitgliedstaats besitzt. Als Ausgangspunkt sollte ein bestimmter Verarbeitungsvorgang für personenbezogene Daten gewählt werden. Bei der Anwendung des Datenschutzrechts auf eine bestimmte Suchmaschine, deren Hauptsitz sich außerhalb des EWR befindet, muss

[12] WP 56, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_de.pdf

die Frage beantwortet werden, ob Niederlassungen im Hoheitsgebiet eines Mitgliedstaats an der Verarbeitung von Benutzerdaten beteiligt sind.

Wie die Arbeitsgruppe bereits in ihrem früheren Arbeitspapier[13] dargelegt hat, setzt eine „Niederlassung" die effektive und tatsächliche Ausübung einer Tätigkeit unter dauerhaften Bedingungen voraus und muss in Übereinstimmung mit der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften bestimmt werden. Die Rechtsform der Niederlassung – eine Geschäftsstelle, eine Tochtergesellschaft mit Rechtspersönlichkeit oder eine Vertretung durch Dritte – ist dabei nicht entscheidend.

Eine weitere Forderung ist jedoch, dass der Verarbeitungsvorgang „im Rahmen der Tätigkeiten" einer Niederlassung ausgeführt wird. Das bedeutet, dass die Niederlassung ebenfalls eine bedeutende Rolle bei dem betreffenden Verarbeitungsvorgang spielen sollte. Dies ist eindeutig der Fall, wenn:

– eine Niederlassung für die Beziehungen zu den Benutzern der Suchmaschine in einem bestimmten gerichtlichen Zuständigkeitsbereich verantwortlich ist;
– ein Suchmaschinenbetreiber ein Büro in einem Mitgliedstaat (EWR) einrichtet, das am Verkauf zielgruppenspezifischer Werbeanzeigen an die Einwohner dieses Staates beteiligt ist;
– die Niederlassung eines Suchmaschinenbetreibers in Bezug auf Benutzerdaten richterlichen Anordnungen und/oder Ersuchen der zuständigen Behörden eines Mitgliedstaats zur Strafverfolgung nachkommt.

Die Verantwortung für die Klärung, inwieweit die Niederlassungen im Hoheitsgebiet der Mitgliedstaaten an der Verarbeitung personenbezogener Daten beteiligt sind, liegt beim Suchmaschinenbetreiber. Ist eine nationale Niederlassung an der Verarbeitung von Benutzerdaten beteiligt, so ist Artikel 4 Absatz 1 Buchstabe a der Datenschutzrichtlinie anwendbar.

Nicht im EWR ansässige Suchmaschinenbetreiber sollten ihre Benutzer darüber informieren, welche Bedingungen – das Vorhandensein einer Niederlassung oder die Verwendung von Mitteln – sie zur Einhaltung der Datenschutzrichtlinie verpflichten.

Verwendung von Mitteln

Suchmaschinen, die im Hoheitsgebiet eines Mitgliedstaats (EWR) für die Verarbeitung von personenbezogenen Daten auf Mittel zurückgreifen, fallen ebenfalls in den Anwendungsbereich der Datenschutzgesetze dieses Mitgliedstaats. Die

[13] WP 56, S. 8, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_de.pdf

Datenschutzgesetze eines Mitgliedstaats sind auch noch anwendbar, wenn der für die Verarbeitung Verantwortliche *„[…] zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, es sei denn, dass diese Mittel nur zum Zweck der Durchfuhr durch das Gebiet der Europäischen Gemeinschaft verwendet werden."*

Was die Bereitstellung von Suchmaschinendiensten außerhalb der EU anbetrifft, so können im Hoheitsgebiet eines Mitgliedstaats befindliche Datenzentren für die Speicherung und Fernverarbeitung personenbezogener Daten genutzt werden. Weitere Beispiele für Mittel sind der Einsatz von Personalcomputern, Endgeräten und Servern. Die Verwendung von Cookies und ähnlichen Softwareinstrumenten durch einen Anbieter von Online-Diensten kann ebenfalls als Rückgriff auf Mittel im Hoheitsgebiet eines Mitgliedstaats angesehen werden, was somit die Anwendung der Datenschutzgesetze des betreffenden Mitgliedstaats erfordert. Dieser Punkt wurde im weiter oben erwähnten Arbeitspapier (WP 56) erörtert: *„Wie bereits gesagt, kann der PC eines Nutzers als ein Mittel im Sinne von Artikel 4 Absatz 1 Buchstabe c der Richtlinie 95/46/EG angesehen werden. Er befindet sich im Gebiet eines Mitgliedstaats. Der für die Verarbeitung Verantwortliche hat beschlossen, dieses Mittel zum Zwecke der Verarbeitung personenbezogener Daten zu nutzen. Wie bereits in den vorstehenden Absätzen erläutert, laufen jetzt einige technische Operationen ab, die nicht unter der Kontrolle der betroffenen Person stehen. Der für die Verarbeitung Verantwortliche verfügt damit über die Mittel des Nutzers und diese Mittel werden nicht nur zum Zwecke der Durchfuhr durch das Gebiet der Gemeinschaft verwendet."*

Schlussfolgerung

Aus der kombinierten Wirkung der Artikel 4 Absatz 1 Buchstabe a und Artikel 4 Absatz 1 Buchstabe c der Datenschutzrichtlinie ergibt sich, dass deren Bestimmungen auf die Verarbeitung personenbezogener Daten durch Suchmaschinenbetreiber in vielen Fällen anwendbar sind, auch wenn sich ihr Hauptsitz außerhalb des EWR befindet.

Welches innerstaatliche Recht in einem bestimmten Fall anwendbar ist, ist Gegenstand einer weiteren Analyse der Fakten des betreffenden Falls. Die Arbeitsgruppe erwartet von den Suchmaschinenbetreibern eine Beteiligung an dieser Analyse, indem sie ihre Rolle und Tätigkeit im EWR in angemessener Weise klären.

Für multinationale Suchmaschinenbetreiber gilt:

– Ein Mitgliedstaat, in dem der Suchmaschinenbetreiber eine Niederlassung besitzt, wendet sein innerstaatliches Datenschutzrecht auf die Verarbeitung gemäß Artikel 4 Absatz 1 Buchstabe a an;

– wenn der Suchmaschinenbetreiber in keinem der Mitgliedstaaten ansässig ist, wendet ein Mitgliedstaat sein innerstaatliches Datenschutzrecht auf die Verarbeitung gemäß Artikel 4 Absatz 1 Buchstabe c an, wenn das Unternehmen im Hoheitsgebiet des Mitgliedstaats[14] zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift (beispielsweise durch Verwendung von Cookies).

In bestimmten Fällen wird ein multinationaler Suchmaschinenbetreiber aufgrund der Regelungen für das anwendbare Recht und der länderübergreifenden Dimension bei der Verarbeitung personenbezogener Daten gleich mehrere Datenschutzgesetze einzuhalten haben:

– Ein Mitgliedstaat wendet sein innerstaatliches Recht auf eine außerhalb des EWR ansässige Suchmaschine an, wenn diese auf Mittel zurückgreift;

– ein Mitgliedstaat kann sein innerstaatliches Recht nicht auf eine im EWR ansässige und einer anderen hoheitsrechtlichen Zuständigkeit unterliegende Suchmaschine anwenden, auch wenn die Suchmaschine auf Mittel zurückgreift. In derartigen Fällen ist das innerstaatliche Recht des Mitgliedstaats anzuwenden, in dem der Suchmaschinenbetreiber niedergelassen ist.

4.1.3. Anwendbarkeit der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und der Richtlinie 2006/24/EG (Richtlinie über die Vorratsspeicherung von Daten)

Suchmaschinendienste im engeren Sinne fallen allgemein nicht unter den neuen Regelungsrahmen für elektronische Kommunikation, zu dem die Datenschutzrichtlinie für elektronische Kommunikation gehört. Artikel 2 Buchstabe c der Rahmenrichtlinie (2002/21/EG), die einige allgemeine Begriffsbestimmungen für den Regelungsrahmen enthält, schließt Dienste ausdrücklich aus, die Inhalte anbieten oder eine redaktionelle Kontrolle über Inhalte ausüben:

„Elektronische Kommunikationsdienste“: gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommmunika-

[14] Bei der Beurteilung, ob Artikel 4 Absatz 1 Buchstabe c in Bezug auf die Verwendung von Cookies geltend gemacht werden kann, legt die Arbeitsgruppe die folgenden Kriterien zugrunde: Das erste Kriterium ist die Situation, in der ein Suchmaschinenbetreiber eine Niederlassung in einem Mitgliedstaat besitzt, Artikel 4 Absatz 1 Buchstabe a aber nicht anwendbar ist, weil diese Niederlassung keine wesentliche Rolle bei der Datenverarbeitung spielt (z. B. ein Pressevertreter). Weitere Kriterien sind die Entwicklung und/oder Gestaltung länderspezifischer Suchmaschinendienste, die tatsächlichen Kenntnisse des Anbieters von Online-Diensten im Umgang mit den Benutzern, die in diesem Land ansässig sind, sowie der Vorteil eines dauerhaften Anteils am Benutzermarkt in einem bestimmten Mitgliedstaat.

tions- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben; nicht dazu gehören die Dienste der Informationsgesellschaft im Sinne von Artikel 1 der Richtlinie 98/34/EG, die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen;

Suchmaschinen fallen somit nicht unter die Definition für elektronische Kommunikationsdienste.

Ein Suchmaschinenbetreiber kann jedoch einen Zusatzdienst anbieten, der unter die Definition für einen elektronischen Kommunikationsdienst fällt, etwa einen öffentlich zugänglichen Dienst für elektronische Post, der der Richtlinie 2002/58/EG für elektronische Kommunikation und der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten unterliegen würde.

In Artikel 5 Absatz 2 der Richtlinie über die Vorratsspeicherung von Daten heißt es ausdrücklich: „Nach dieser Richtlinie dürfen keinerlei Daten, die Aufschluss über den Inhalt einer Kommunikation geben, auf Vorrat gespeichert werden." Demzufolge wären Suchanfragen als Inhaltsdaten und nicht als Verkehrsdaten zu qualifizieren, und die Richtlinie würde ihre Speicherung auf Vorrat somit nicht rechtfertigen.

Jegliche Bezugnahmen auf die Richtlinie über die Vorratsspeicherung von Daten in Verbindung mit der Speicherung von Server-Protokollen, die von einem Suchmaschinendienst generiert werden, gehen folglich fehl.

Artikel 5 Absatz 3 und Artikel 13 der Datenschutzrichtlinie für elektronische Kommunikation

Einige Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation wie Artikel 5 Absatz 3 (Cookies und Spyware) und Artikel 13 (unerbetene Nachrichten) sind allgemeine Bestimmungen, die nicht nur auf die elektronische Kommunikationsdienste anwendbar sind, sondern auch auf andere Dienste, in denen diese Techniken verwendet werden.

Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation, die im Zusammenhang mit Erwägungsgrund 25 dieser Richtlinie zu lesen ist, befasst sich mit der Speicherung von Informationen im Endgerät eines Teilnehmers oder Nutzers. Die Verwendung dauerhafter Cookies mit eindeutigen Kennungen bietet die Möglichkeit, die Nutzung eines bestimmten Computers zu verfolgen und ein entsprechendes Profil zu erstellen, selbst wenn dynamische IP-Adressen verwendet werden. Artikel 5 Absatz 3 und Erwägungsgrund 25 der Datenschutzrichtlinie für elektronische Kommunikation legen eindeutig dar, dass die Spei-

cherung derartiger Informationen im Endgerät der Nutzer, d. h. Cookies und ähnliche Instrumente (kurz: Cookie), im Einklang mit den Bestimmungen der Datenschutzrichtlinie stehen muss. Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation klärt somit die Verpflichtungen hinsichtlich der Verwendung von Cookies durch einen Dienst der Informationsgesellschaft aufgrund der Datenschutzrichtlinie.

4.2. Anbieter von Inhalten

Die Suchmaschinen verarbeiten Informationen, einschließlich personenbezogener Daten, indem sie das Internet und andere Quellen, die sie durchsuchbar und durch diese Dienste einfach zugänglich machen, durchforsten, analysieren und indexieren. Einige Suchmaschinendienste veröffentlichen Daten in einem so genannten „Cache“ (Zwischenspeicher) neu.

4.2.1. Freie Meinungsäußerung und Recht auf Privatsphäre

Die Arbeitsgruppe ist sich der besonderen Rolle von Suchmaschinen in der Online-Informationsumgebung bewusst. Beim gemeinschaftlichen Datenschutzrecht und bei den Rechtsvorschriften der verschiedenen Mitgliedstaaten geht es darum, ein Gleichgewicht zwischen dem Schutz des Rechts auf Privatsphäre und dem Schutz personenbezogener Daten einerseits und dem ungehinderten Informationsfluss und dem Grundrecht auf freie Meinungsäußerung andererseits zu finden.

Artikel 9 der Datenschutzrichtlinie soll garantieren, dass dieses Gleichgewicht in den Rechtsvorschriften der Mitgliedstaaten im Kontext der Medien gefunden wird. Außerdem hat der Europäische Gerichtshof klargestellt, dass die Grenzen der freien Meinungsäußerung, die sich aus der Anwendung der Datenschutzgrundsätze ableiten, mit dem geltenden Recht im Einklang stehen und den Grundsatz der Verhältnismäßigkeit beachten müssen.[15]

4.2.2. Datenschutzrichtlinie

Die Datenschutzrichtlinie enthält keine spezielle Bezugnahme auf die Verarbeitung personenbezogener Daten durch Dienste der Informationsgesellschaft, die als Vermittler handeln. Das entscheidende Kriterium in der Datenschutzrichtlinie

[15] Der Europäische Gerichtshof hat zur Verhältnismäßigkeit der Wirkung der Datenschutzbestimmungen, d. h. zur freien Meinungsäußerung, in seinem Urteil in der Rechtssache Lindqvist gegen Schweden, Randnr. 88–90, ausführlich Stellung bezogen.

(95/46/EG) für die Anwendbarkeit der Datenschutzbestimmungen ist die Definition des für die Verarbeitung Verantwortlichen, nämlich ob eine bestimmte Stelle „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Die Frage, ob ein Vermittler als der eigentliche für die Verarbeitung Verantwortliche anzusehen ist, oder aber als eine Stelle, die gemeinsam mit anderen für eine bestimmte Verarbeitung von personenbezogenen Daten verantwortlich ist, ist getrennt von der Frage der Haftung für eine derartige Verarbeitung zu betrachten.[16]

Nach dem Grundsatz der Verhältnismäßigkeit ist ein Suchmaschinenbetreiber, der ausschließlich als Vermittler handelt, nicht als der Hauptverantwortliche für die inhaltliche Verarbeitung von personenbezogenen Daten anzusehen. In diesem Fall liegt die Hauptverantwortung für die Verarbeitung von personenbezogenen Daten beim Informationsanbieter.[17] Die formale, rechtliche und praktische Kontrolle des Suchmaschinenbetreibers über die personenbezogenen Daten beschränkt sich in der Regel auf die Möglichkeit, Daten von ihren Servern zu entfernen. Was die Entfernung von personenbezogenen Daten aus ihrem Index und ihren Suchergebnissen anbetrifft, so verfügen die Suchmaschinenbetreiber über eine ausreichende Kontrolle, um sie hier als für die Verarbeitung Verantwortliche (allein oder gemeinsam mit anderen) anzusehen. In welchem Umfang sie jedoch zur Entfernung oder Sperrung von personenbezogenen Daten verpflichtet sind, hängt womöglich vom allgemeinen Deliktrecht und von den Haftungsvorschriften des jeweiligen Mitgliedstaats ab.[18]

Eigentümer von Websites können mit Hilfe der Datei *robots.txt* oder der Merker *Noindex/NoArchive* von Vornherein ihre Nichtbeteiligung („Opt-out") an Suchmaschinen und an der Zwischenspeicherung erklären.[19] Es ist sehr wichtig, dass

---

[16] In einigen Mitgliedstaaten gibt es spezielle Ausnahmeregelungen auf horizontaler Ebene („sichere Häfen") in Bezug auf die Haftung von Suchmaschinen („Instrumente zur Lokalisierung von Informationen"). Die Richtlinie über den elektronischen Geschäftsverkehr (2000/31/EG) sieht zwar keine sicheren Häfen für Suchmaschinen vor, doch wurden in einigen Mitgliedstaaten dennoch entsprechende Regelungen umgesetzt. Siehe dazu „Erster Bericht über die Anwendung der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr")", 21.11.2003, KOM(2003) 702 endg., S. 13.

[17] Streng genommen könnten die Benutzer des Suchmaschinendienste ebenfalls als für die Verarbeitung Verantwortliche angesehen werden, doch ihre Rolle liegt als „ausschließlich persönliche Tätigkeit" in der Regel außerhalb des Anwendungsbereichs der Richtlinie (siehe Artikel 3 Absatz 2, zweiter Spiegelstrich).

[18] In einigen EU-Mitgliedstaaten haben die Datenschutzbehörden spezielle Regelungen für die Verantwortlichkeit von Suchmaschinenbetreibern erlassen, Inhaltsdaten vom Suchindex zu entfernen. Diese Regelungen beruhen auf dem in Artikel 14 der Datenschutzrichtlinie (95/46/EG) verankerten Widerspruchsrecht und auf der Richtlinie über den elektronischen Geschäftsverkehr (2000/31/EG). Gemäß diesen einzelstaatlichen Rechtsvorschriften sind die Suchmaschinenbetreiber verpflichtet, ein Verfahren zur Meldung und Entfernung rechtswidriger Inhalte ähnlich wie Hosting-Anbieter einzuhalten, damit sie von der Haftung freigestellt bleiben.

[19] Dies kann mehr als eine optionale Lösung sein. Veröffentlicher von personenbezogenen Daten müssen sich mit der Frage befassen, ob ihre Rechtsgrundlage für die Veröffentlichung die Indexierung dieser Informationen durch Suchmaschinen einschließt, und gegebenenfalls entsprechende Schutzmechanismen vorsehen, unter anderem durch Verwendung der Datei robots.txt und/oder Noindex/NoArchive-Merker.

die Suchmaschinenbetreiber derartigen Nichtbeteiligungsklauseln von Website-Herausgebern Beachtung schenken. Diese Nichtbeteiligung kann vor der ersten Durchsuchung („Crawling“) der Website oder auch nach ihrer Durchsuchung angegeben werden; im zuletzt genannten Fall sollte die Suchmaschine so schnell wie möglich einen Aktualisierungslauf durchführen.

Suchmaschinenbetreiber beschränken sich nicht immer auf eine reine Vermittlertätigkeit. Beispielsweise speichern einige Suchmaschinen komplette Web-Inhalte – einschließlich der darin enthaltenen personenbezogenen Daten – auf ihren Servern. Außerdem ist unklar, inwieweit die Suchmaschinen in den von ihnen verarbeiteten Inhalten aktiv nach personenbezogenen Daten suchen. Die Durchsuchung, Analyse und Indexierung kann automatisch erfolgen, ohne das Vorhandensein von personenbezogenen Daten zu offenbaren. Spezielle Arten von personenbezogenen Daten wie beispielsweise Sozialversicherungsnummern, Kreditkartennummern, Telefonnummern und Adressen für elektronische Post können aufgrund ihres Formats jedoch einfach ermittelt werden. Es gibt aber auch höher entwickelte Technologien, die von den Suchmaschinenbetreibern in zunehmendem Maße eingesetzt werden. Dazu gehören beispielsweise die Technologie zur Gesichtserkennung im Zusammenhang mit der Bildverarbeitung und Bildsuche.

Auf diese Weise können die Suchmaschinenbetreiber Mehrwert schaffende Vorgänge durchführen, die mit den Merkmalen oder Arten von personenbezogenen Daten in den verarbeiteten Informationen verknüpft sind. In diesen Fällen trägt der Suchmaschinenbetreiber im Rahmen der Datenschutzgesetze die volle Verantwortung für den Inhalt, der aus der Verarbeitung personenbezogener Daten resultiert. Die gleiche Verantwortlichkeit gilt für einen Suchmaschinenbetreiber, der Werbeanzeigen verkauft, die aufgrund personenbezogener Daten – beispielsweise des Namens einer Person – geschaltet werden.

Die Caching-Funktionalität

Die Caching-Funktionalität ist eine weitere Möglichkeit für Suchmaschinenbetreiber, über ihre Rolle als reine Informationsvermittler hinauszugehen. Die Speicherungsfrist von Inhalten in einem Cache-Speicher sollte auf den Zeitraum begrenzt werden, der zur Lösung des Problems der vorübergehenden Nichtverfügbarkeit der eigentlichen Website notwendig ist.

Jegliche Zwischenspeicherung von auf indexierten Websites enthaltenen, personenbezogenen Daten über diesen aus Gründen der technischen Verfügbarkeit notwendigen Zeitraum hinaus ist als eine unabhängige Neuveröffentlichung anzusehen. Nach Auffassung der Arbeitsgruppe liegt die Verantwortung für die Einhaltung der Datenschutzgesetze hier beim Anbieter derartiger Caching-Funktionalitäten in seiner Rolle als Verantwortlicher für die Verarbeitung der personenbe-

zogenen Daten, die in den zwischengespeicherten Veröffentlichungen enthalten sind. Falls die ursprüngliche Veröffentlichung geändert wird, etwa um unrichtige personenbezogene Daten zu entfernen, sollte der Verantwortliche für die Verarbeitung der Cache-Inhalte umgehend auf Aufforderungen zur Aktualisierung des Cache-Kopie reagieren oder die Cache-Kopie vorübergehend sperren, bis die Website von der Suchmaschine erneut durchsucht wird.

5. RECHTMÄSSIGKEIT DER VERARBEITUNG

Artikel 6 der Datenschutzrichtlinie sieht vor, dass personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden, für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Außerdem müssen die verarbeiteten Daten den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen. Damit die Verarbeitung personenbezogener Daten rechtmäßig ist, muss gemäß Artikel 7 dieser Richtlinie mindestens eine der sechs Voraussetzungen für die Zulässigkeit der Verarbeitung erfüllt sein.

5.1. Von den Suchmaschinenbetreibern vorgebrachte Zwecke und Gründe

Für die Verwendung und Speicherung von personenbezogenen Daten führen die Suchmaschinenbetreiber in ihrer Rolle als für die Verarbeitung Verantwortliche allgemein die folgenden Zwecke und Gründe an.

Verbesserung des Dienstes

Viele Suchmaschinenbetreiber verwenden Server-Protokolle, um ihr Dienstleistungsangebot und die Qualität ihrer Suchdienste zu verbessern. Sie sehen die Auswertung der Server-Protokolle als ein wichtiges Instrument, um die Qualität der Suchvorgänge, Ergebnisse und Werbung zu verbessern und neue, noch nicht näher bestimmbare Dienste zu entwickeln.

Systemsicherheit

Server-Protokolle tragen nach Auskunft der Betreiber zur Sicherheit der Suchmaschinendienste bei. Einige Suchmaschinenbetreiber erklärten, dass die Speicherung von Protokollen zum Schutz des Systems vor Sicherheitsangriffen beitragen kann und eine aussagekräftige Stichprobe an Server-Protokolldaten notwendig ist, um wiederkehrende Muster zu erkennen und Sicherheitsbedrohungen zu analysieren.

Betrugsbekämpfung

Server-Protokolle schützen die Systeme und Benutzer der Suchmaschinen angeblich vor Betrug und Missbrauch. Viele Suchmaschinenbetreiber betreiben einen „Pay-per-Click"-Mechanismus für die angezeigte Werbung. Ein Nachteil dieses Systems ist jedoch, dass einem Unternehmen zu Unrecht Gebühren in Rechnung gestellt werden können, wenn ein Angreifer mit Hilfe automatischer Software systematisch auf die Werbeanzeigen klickt. Die Suchmaschinenbetreiber achten zunehmend darauf, dass ein derartiges Verhalten aufgedeckt und beseitigt wird.

Abrechnungsanforderungen werden als Zweck für Dienste wie Klicks auf gesponserte Links angeführt, wenn aus Abrechnungsgründen eine vertragliche Verpflichtung zur Datenspeicherung besteht, und zwar mindestens bis zur Begleichung der Rechnungen und bis zum Ablauf der Frist für Rechtsstreitigkeiten.

Personalisierte Werbung

Zur Erhöhung ihrer Einnahmen streben die Suchmaschinenbetreiber eine personalisierte Werbung an. Gegenwärtig werden unter anderem die bisherigen Suchanfragen, Benutzerkategorien sowie geografische Kriterien berücksichtigt. Daher kann auf Basis des bisherigen Benutzerverhaltens und der IP-Adresse des Benutzers personalisierte Werbung angezeigt werden.

Einige Suchmaschinen erstellen auch Statistiken um zu bestimmen, welche Benutzerkategorien auf welche Informationen zu welcher Zeit online zugreifen. Diese Daten können für die Verbesserung der Dienste, für zielgruppenspezifische Werbung sowie für kommerzielle Zwecke verwendet werden, um die Kosten für ein Unternehmen zu ermitteln, das für seine Produkte im Internet werben möchte.

Strafverfolgung

Nach Angaben einiger Betreiber stellen Protokolle ein wichtiges Instrument für die Strafverfolgung dar, um schwere Straftaten wie Kindesmissbrauch untersuchen und strafrechtlich verfolgen zu können.

5.2. Analyse der Zwecke und Gründe durch die Arbeitsgruppe

Generell ist festzustellen, dass die Suchmaschinenbetreiber keinen umfassenden Überblick geben, für welche festgelegten, eindeutigen und rechtmäßigen Zwecke sie personenbezogene Daten verarbeiten. Erstens sind einige Zwecke wie „Verbesserung der Dienste" oder „personalisierte Werbung" zu allgemein definiert und bieten daher keinen angemessenen Beurteilungsrahmen für die Rechtmäßig-

keit der Zwecke. Da zahlreiche Suchmaschinenbetreiber viele verschiedene Verarbeitungszwecke anführen, ist zweitens nicht klar, in welchem Umfang Daten für einen anderen Zweck weiterverarbeitet werden, der mit der ursprünglichen Zweckbestimmung nicht vereinbar ist.

Die Erhebung und Verarbeitung von personenbezogenen Daten kann unter einer oder mehreren Voraussetzungen rechtmäßig sein. Es gibt drei Gründe, auf die sich die Suchmaschinenbetreiber für verschiedene Zwecke berufen können.

– Einwilligung – Artikel 7 Buchstabe a der Datenschutzrichtlinie

Die Dienste der meisten Suchmaschinenbetreiber können sowohl ohne als auch mit Registrierung genutzt werden. Im zweiten Fall (wenn ein Benutzer beispielsweise ein spezifisches Benutzerkonto angelegt hat) kann die Einwilligung[20] als zulässiger Grund für die Verarbeitung bestimmter, festgelegter Kategorien von personenbezogenen Daten für festgelegte, rechtmäßige Zwecke, einschließlich der Speicherung der Daten für einen begrenzten Zeitraum, angeführt werden. Bei anonymen Benutzern des Dienstes und den personenbezogenen Daten von Benutzern, die sich gegen eine freiwillige Authentifizierung entschieden haben, kann freilich nicht von einer Einwilligung ausgegangen werden. Derartige Daten dürfen nicht für Zwecke verarbeitet oder gespeichert werden, die über die Anzeige einer Liste von Suchergebnissen für eine spezifische Suchanfrage hinausgehen.

– Erforderlich für die Erfüllung eines Vertrags – Artikel 7 Buchstabe b der Datenschutzrichtlinie

Eine Verarbeitung kann auch erforderlich sein für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen. Auf diese Rechtsgrundlage können sich Suchmaschinenbetreiber bei der Erhebung von personenbezogenen Daten berufen, die ein Benutzer freiwillig angibt, um sich bei einem bestimmten Dienst, beispielsweise bei einem Benutzerkonto, anzumelden. Ähnlich wie im Falle der Einwilligung kann diese Rechtsgrundlage für die Verarbeitung bestimmter, festgelegter Kategorien von personenbezogenen Daten für festgelegte, rechtmäßige Zwecke von authentifizierten Benutzern angeführt werden.

Viele Internet-Unternehmen machen auch geltend, dass ein Benutzer bei der Nutzung der auf ihrer Website angebotenen Dienste, wie beispielsweise einer Such-

[20] Gemäß Artikel 2 Buchstabe h der Datenschutzrichtlinie ist die Einwilligung der betroffenen Person „jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden."

maske, faktisch eine vertragliche Beziehung eingeht. Eine derartige generelle Annahme erfüllt jedoch nicht die strenge Begrenzung auf die Erforderlichkeit, die in der Richtlinie gefordert wird.[21]

– Erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen wahrgenommen wird – Artikel 7 Buchstabe f der Datenschutzrichtlinie

Gemäß Artikel 7 Buchstabe f der Richtlinie könnte die Verarbeitung zur Verwirklichung des berechtigten Interesses erforderlich sein, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiegen.

Verbesserung der Dienste

Einige Suchmaschinenbetreiber speichern den Inhalt von Benutzeranfragen in ihren Server-Protokollen. Diese Informationen stellen ein wichtiges Instrument für Suchmaschinenbetreiber dar. Sie ermöglichen ihnen die Verbesserung ihrer Dienste durch die Analyse der Art von Suchanfragen und deren Verfeinerung und durch die Auswertung der von den Benutzern weiterverfolgten Suchergebnisse. Die Artikel-29-Arbeitsgruppe hält die Zuordnung der Suchanfragen zu identifizierbaren Personen jedoch nicht für zwingend erforderlich, damit die Betreiber ihre Suchdienste verbessern können.

Um die Aktionen eines einzelnen Benutzers zu korrelieren (und auf diese Weise z. B. zu ermitteln, ob die Vorschläge der Suchmaschine hilfreich sind), ist lediglich eine Abgrenzung der Aktionen eines Benutzers bei einer bestimmten Suchanfrage von denen eines anderen Benutzers notwendig; die Identifizierung dieser Benutzer ist hingegen nicht notwendig. Beispielsweise könnte für eine Suchmaschine die Information aufschlussreich sein, dass Benutzer X nach „Woodhouse“ gesucht und anschließend auf die Ergebnisse für die angebotene orthografische Variante „Wodehouse“ geklickt hat – sie braucht aber nicht zu wissen, wer Benutzer X ist. Die Verbesserung der Dienste kann daher nicht als zulässiger Grund für die Speicherung nicht anonymisierter Daten angesehen werden.

Systemsicherheit

Die Suchmaschinenbetreiber könnten die Notwendigkeit zur Aufrechterhaltung der Sicherheit ihres Systems als berechtigtes Interesse und angemessenen Grund

[21] Artikel 7 Buchstabe b der Richtlinie: „… erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen.“

für die Verarbeitung personenbezogener Daten anführen. Personenbezogene Daten, die für Sicherheitszwecke gespeichert werden, müssen jedoch einer strengen Zweckbeschränkung unterliegen. Daher dürfen Daten, die für Sicherheitszwecke gespeichert werden, nicht für andere Zwecke, beispielsweise zur Optimierung eines Dienstes, verwendet werden. Die Suchmaschinenbetreiber argumentieren, dass die Speicherung der Server-Protokolle über einen angemessenen Zeitraum (die Anzahl der Monate ist von Suchmaschine zu Suchmaschine unterschiedlich) notwendig ist, damit sie typische Verhaltensmuster der Benutzer erkennen und folglich Überflutungsangriffe („Denial of Service“) und andere Sicherheitsbedrohungen ermitteln und abwehren können. Alle Suchmaschinenbetreiber sollten jedoch in der Lage sein, die gewählte Speicherungsfrist für diesen Zweck und die damit einhergehende Notwendigkeit zur Verarbeitung dieser Daten umfassend zu begründen.

Betrugsbekämpfung

Trotz des berechtigten Interesses der Suchmaschinenbetreiber an der Erkennung und Vermeidung von Betrugsdelikten wie etwa „Klick-Betrug“ sollte ebenso wie bei der Speicherung für Sicherheitszwecke die Menge der gespeicherten und verarbeiteten personenbezogenen Daten und die für diesen Zweck angesetzte Speicherungsfrist für personenbezogene Daten davon abhängen, ob die Daten für die Erkennung und Vermeidung von Betrugsdelikten tatsächlich notwendig sind.

Abrechnung

Die systematische Protokollierung üblicher Suchmaschinendaten, in denen der Benutzer nicht auf einen gesponserten Link geklickt hat, kann nicht mit Abrechnungsanforderungen gerechtfertigt werden. Ausgehend von den Antworten der Suchmaschinenbetreiber auf den Fragebogen hat die Arbeitsgruppe auch erhebliche Zweifel, dass personenbezogene Daten von Suchmaschinenbenutzern für Abrechnungszwecke wirklich notwendig sind. Für eine schlüssige Beurteilung wären weitere Untersuchungen notwendig. Auf jeden Fall fordert die Arbeitsgruppe die Suchmaschinenbetreiber zur Entwicklung von Abrechnungsmechanismen auf, die mehr Rücksicht auf die Privatsphäre nehmen, beispielsweise durch Verwendung anonymisierter Daten.

Personalisierte Werbung

Suchmaschinenbetreiber, die personalisierte Werbung zur Steigerung ihrer Einnahmen anbieten möchten, können die Rechtmäßigkeit der Verarbeitung einiger personenbezogener Daten zwar mit Artikel 7 Buchstabe a der Richtlinie (Einwilligung) oder Artikel 7 Buchstabe b der Richtlinie (Erfüllung eines Vertrags) begründen, doch es ist schwierig, einen rechtmäßigen Grund für diese Praxis bei Benutzern zu finden, die nicht ihre ausdrückliche Einwilligung auf der Grund-

lage spezifischer Informationen über den Verarbeitungszweck gegeben haben. Die Arbeitsgruppe spricht sich eindeutig für anonymisierte Daten aus.

Strafverfolgung und Rechtsersuchen

Gelegentlich fordern Strafverfolgungsbehörden Benutzerdaten von Suchmaschinen an, um Straftaten aufzudecken oder zu verhindern. Auch Privatparteien könnten versuchen, einen Suchmaschinenbetreiber über eine richterliche Anordnung zur Herausgabe von Benutzerdaten zu veranlassen. Sofern derartige Rechtsersuchen die geltenden Rechtsverfahren einhalten und zu rechtsgültigen gerichtlichen Anordnungen führen, müssen Suchmaschinenbetreiber diese selbstverständlich befolgen und die benötigten Informationen liefern. Diese Einhaltung von Anordnungen sollte jedoch nicht mit einer rechtlichen Verpflichtung oder Rechtfertigung für die Speicherung derartiger Daten ausschließlich für diese Zwecke verwechselt werden.

Außerdem könnten große Bestände an personenbezogenen Daten in den Händen der Suchmaschinenbetreiber die Strafverfolgungsbehörden und andere Kreise dazu verleiten, ihre Rechte häufiger und mit mehr Nachdruck auszuüben, was wiederum zu einem Vertrauensverlust bei den Verbrauchern führen könnte.

5.3. Von der Branche zu klärende Fragen

Speicherungsfristen

Wenn die vom Suchmaschinenbetreiber durchgeführte Verarbeitung dem einzelstaatlichen Recht unterliegt, müssen dabei die Rechtsvorschriften des betreffenden Mitgliedstaats für den Schutz der Privatsphäre und die Speicherungsfristen eingehalten werden.

Bei der Speicherung personenbezogener Daten sollte die Speicherungsfrist nicht über den für die spezifischen Verarbeitungszwecke notwendigen Zeitraum hinausgehen. Folglich könnten am Ende einer Suchsitzung die personenbezogenen Daten gelöscht werden; eine fortgesetzte Speicherung müsste dann angemessen begründet werden. Einige Suchmaschinenbetreiber scheinen Daten jedoch auf unbestimmte Zeit zu speichern, was verboten ist. Für jeden Zweck sollte eine befristete Speicherungsdauer festgelegt werden. Außerdem sollte die zu speichernde Menge an personenbezogenen Daten nicht über den jeweiligen Zweck hinausgehen.

In der Praxis speichern die großen Suchmaschinenbetreiber die personenbezogenen Daten über ihre Benutzer in aller Regel über ein Jahr lang (die genauen Zeiten können abweichen). Die Arbeitsgruppe begrüßt die jüngsten Reduzierungen

der Speicherungsfristen für personenbezogene Daten durch große Suchmaschinenbetreiber. Die Tatsache, dass führende Unternehmen in dieser Branche ihre Speicherungsfristen reduzieren konnten, deutet freilich darauf hin, dass die bisherigen Fristen länger als notwendig waren.

Angesichts der bisher abgegebenen Stellungnahmen der Suchmaschinenbetreiber zu den möglichen Zwecken für die Erhebung personenbezogener Daten sieht die Arbeitsgruppe keine Grundlage für eine Speicherungsfrist von mehr als sechs Monaten.[22]

Die Speicherung von personenbezogenen Daten und die entsprechende Speicherungsfrist müssen immer (mit konkreten und relevanten Argumenten) begründbar sein und auf ein Minimum reduziert werden, um die Transparenz zu verbessern, eine Verarbeitung nach Treu und Glauben sicherzustellen und die Verhältnismäßigkeit für den Zweck zu gewährleisten, der eine derartige Speicherung rechtfertigt.

Daher fordert die Arbeitsgruppe die Suchmaschinenbetreiber dazu auf, den Grundsatz „Privacy by Design" (entwurfsimmanenter Schutz der Privatsphäre) zu verwirklichen, der zur weiteren Reduzierung der Speicherungsfrist beitragen wird. Nach Auffassung der Arbeitsgruppe wird eine reduzierte Speicherungsfrist das Vertrauen der Benutzer in den Dienst stärken und folglich einen wichtigen Wettbewerbsvorteil darstellen.

Falls die Suchmaschinenbetreiber personenbezogene Daten länger als sechs Monate speichern, müssen sie umfassend nachweisen, dass dies für den Dienst zwingend notwendig ist.

In jedem Fall müssen die Suchmaschinenbetreiber die Benutzer über ihre jeweilige Speicherungspolitik für alle Arten der von ihnen verarbeiteten Benutzerdaten informieren.

Weiterverarbeitung für verschiedene Zwecke

In welchem Umfang und wie Benutzerdaten weiter analysiert und ob (detaillierte) Benutzerprofile erstellt werden, hängt vom Suchmaschinenbetreiber ab. Die Arbeitsgruppe ist sich der Möglichkeit bewusst, dass diese Art der Weiterverarbeitung von Benutzerdaten womöglich einen Kernbereich der Innovation der Suchmaschinentechnologie berührt und für den Wettbewerb von großer Bedeutung sein kann. Die uneingeschränkte Offenlegung der Weiterverwendung und Analyse von Benutzerdaten könnte auch die Anfälligkeit der Suchmaschinendienste für den Missbrauch ihrer Dienste erhöhen. Derlei Erwägungen kön-

[22] In den einzelstaatlichen Rechtsvorschriften kann die Löschung von personenbezogenen Daten auch zu einem früheren Zeitpunkt vorgeschrieben sein.

nen jedoch nicht als Rechtfertigung für die Nichteinhaltung der anwendbaren Datenschutzgesetze der Mitgliedstaaten geltend gemacht werden. Außerdem können sich die Suchmaschinenbetreiber nicht darauf berufen, dass sie mit der Erhebung von personenbezogenen Daten die Entwicklung neuer Dienste bezwecken, deren genaue Art noch nicht feststeht. Aus Gründen der Fairness sollten die betroffenen Personen über den Umfang der möglichen Eingriffe in ihre Privatsphäre Bescheid wissen, wenn jemand Kenntnis von ihren Daten erlangt. Dies wird aber nicht möglich sein, wenn die Zwecke nicht genauer definiert werden.

Cookies

Dauerhafte Cookies mit einer eindeutigen Benutzerkennung sind personenbezogene Daten und unterliegen daher den anwendbaren Datenschutzgesetzen. Die Verantwortung für deren Verarbeitung kann nicht auf die Verantwortung des Benutzers reduziert werden, bestimmte Vorsichtsmaßnahmen in seinen Browser-Einstellungen zu treffen. Der Suchmaschinenbetreiber entscheidet darüber, ob ein Cookie gespeichert wird, welcher Cookie gespeichert wird und für welche Zwecke er verwendet wird. Auch das von einigen Suchmaschinenbetreibern eingestellte Verfallsdatum von Cookies erscheint übermäßig lang. Beispielsweise setzen verschiedene Unternehmen Cookies, die erst nach vielen Jahren verfallen. Bei Verwendung eines Cookies sollte für das Cookie eine angemessene Lebensdauer gewählt werden, die zum einen ein verbessertes Surf-Erlebnis und zum anderen eine Befristung der Lebensdauer ermöglicht. Vor allem im Hinblick auf die Standardeinstellungen von Browsern ist es sehr wichtig, dass die Benutzer umfassend über die Verwendung und die Wirkung von Cookies informiert werden. Diese Information sollte stärker in den Vordergrund gerückt werden und nicht nur ein Bestandteil der Datenschutzerklärungen sein, die in der Suchmaschine nicht unbedingt auf Anhieb auffindbar sind.

Anonymisierung

Wenn es keinen rechtmäßigen Grund für die Verarbeitung bzw. für die Verwendung über die festgelegten rechtmäßigen Zwecke hinaus gibt, müssen die Suchmaschinenbetreiber die personenbezogenen Daten löschen. Statt die Daten zu löschen, können sie sie auch anonymisieren. Diese Anonymisierung muss jedoch vollständig unumkehrbar sein, damit die Datenschutzrichtlinie nicht länger greift.

Selbst dort, wo eine IP-Adresse und ein Cookie durch eine eindeutige Kennung ersetzt werden, ist die Identifizierung von Personen durch Korrelation von gespeicherten Suchanfragen möglich. Aus diesem Grund sollten dort, wo eine Anonymisierung statt Löschung der Daten erfolgt, die verwendeten Methoden sorgfältig geprüft und gründlich durchgeführt werden. Dies kann die Beseitigung von Teilen der Suchhistorie erfordern, um die Möglichkeit einer indirekten Identifizierung des Benutzers auszuschließen, der diese Suchvorgänge durchgeführt hat.

Bei der Anonymisierung von Daten sollte jegliche Möglichkeit der Identifizierung von Personen ausgeschlossen werden. Auszuschließen ist selbst das Kombinieren der anonymisierten Informationen eines Suchmaschinenbetreibers mit Informationen, die ein anderer Beteiligter gespeichert hat (beispielsweise ein Internet-Diensteanbieter). Derzeit schneiden einige Suchmaschinenbetreiber IPv4-Adressen ab, indem sie die letzte Achtergruppe entfernen, womit sie effektiv Informationen über den Internet-Diensteanbieter oder das Teilnetz des Benutzers speichern, ohne die Person direkt zu identifizieren. Die Aktivität könnte dann von einer beliebigen der 254 IP-Adressen ausgehen. Dies ist für eine Anonymisierungsgarantie möglicherweise aber nicht immer ausreichend.

Zudem muss die Anonymisierung oder Löschung der Protokolle rückwirkend erfolgen und alle relevanten Protokolle der Suchmaschine weltweit einschließen.

Dienstübergreifende Datenkorrelation

Viele Suchmaschinenbetreiber bieten den Benutzern die Möglichkeit, die Nutzung der Dienste über ein persönliches Konto zu personalisieren. Abgesehen von Suchfunktionen bieten sie Dienste wie elektronische Post und/oder andere Kommunikationswerkzeuge, wie beispielsweise Boten (Messenger) oder Chats, und soziale Vernetzungsinstrumente wie Internet-Tagebücher (Web-Blogs) oder soziale Communities. Das entsprechende Angebot kann zwar von Anbieter zu Anbieter unterschiedlich sein, doch ein gemeinsames Merkmal derartiger Dienste ist das ihnen zugrunde liegende Geschäftsmodell und die kontinuierliche Entwicklung neuer personalisierter Dienste.

Die Korrelation des Kundenverhaltens über verschiedene personalisierte Dienste eines Suchmaschinenbetreibers und mitunter auch über verschiedene Plattformen[23] hinweg wird aus technischer Sicht durch die Benutzung eines zentralen persönlichen Kontos erleichtert, kann aber auch durch andere Mittel auf Basis von Cookies oder anderen charakteristischen Merkmalen wie einzelnen IP-Adressen bewerkstelligt werden. Wenn eine Suchmaschine beispielsweise einen Zusatzdienst wie „Desktop-Suche“ anbietet, erhält die Suchmaschine Informationen über die (Inhalte der) Dokumente, die ein Benutzer erstellt oder anzeigt. Mit Hilfe dieser Daten können die Suchanfragen angepasst werden und genauere Ergebnisse liefern.

Nach Auffassung der Arbeitsgruppe ist das dienst- und plattformübergreifende Korrelieren von personenbezogenen Daten für authentifizierte Benutzer nur mit Einwilligung und nach angemessener Unterrichtung der Benutzer rechtmäßig.

[23] Beispielsweise bei Microsoft von der webbasierten Suchmaschine bis hin zu der mit dem Internet verbundenen Hardware, die für Spielzwecke verkauft wird (Xbox).

Wenn ein Benutzer die Vorteile eines stärker personalisierten Suchdienstes nutzen möchte, sollte die Registrierung bei einem Suchmaschinenbetreiber freiwillig sein. Die Suchmaschinenbetreiber dürfen den Benutzer nicht zu der Annahme verleiten, dass die Nutzung ihres Dienstes ein personalisiertes Konto erfordert, indem sie nicht identifizierte Benutzer automatisch zu einem Anmeldeformular für ein personalisiertes Konto umleiten, da keine Notwendigkeit und somit auch kein zulässiger Grund für die Erhebung derartiger personenbezogenen Daten besteht, außer mit freier Willenserklärung des Benutzers.

Eine Korrelation kann auch bei nicht authentifizierten Benutzern auf Basis von IP-Adressen oder eindeutigen Cookies erfolgen, die von allen verschiedenen Diensten eines Suchmaschinenbetreibers erkannt werden können. Gewöhnlich geschieht dies automatisch, ohne dass sich der Benutzer einer derartigen Korrelation bewusst ist. Die heimliche Überwachung des Benutzerverhaltens und sicherlich auch privaten Verhaltens wie der Besuch von Websites steht nicht im Einklang mit den Grundsätzen einer rechtmäßigen Verarbeitung nach Treu und Glauben im Sinne der Datenschutzrichtlinie. Die Suchmaschinenbetreiber sollten sich klar zum Umfang der dienstübergreifenden Korrelation von Daten äußern und Korrelationen nur mit Einwilligung des Benutzers vornehmen.

Einige Suchmaschinenbetreiber räumen in ihren Datenschutzerklärungen ausdrücklich ein, dass sie die vom Benutzer bereitgestellten Daten mit Daten von Dritten anreichern, z. B. von anderen Unternehmen, die beispielsweise geografische Informationen an Bereiche von IP-Adressen oder Websites mit Werbeanzeigen anhängen, die vom Suchmaschinenbetreiber verkauft werden.[24] Diese Art der Korrelation kann rechtswidrig sein, wenn die betroffenen Personen bei der Erhebung ihrer personenbezogenen Daten nicht informiert werden und wenn ihnen keine einfachen Zugriffsmöglichkeiten auf ihre Personenprofile und das Recht auf Berichtigung oder Löschung bestimmter unrichtiger oder überflüssiger Datenelemente eingeräumt wird. Ist die betreffende Verarbeitung für die Bereitstel-

[24] Beispielsweise weist Microsoft in seiner Online-Datenschutzerklärung auf Folgendes hin: „Bei der Registrierung für bestimmte Microsoft-Dienste werden Sie nach persönlichen Informationen gefragt. Die von uns erfassten Daten werden möglicherweise mit Informationen kombiniert, die von anderen Microsoft-Diensten oder anderen Unternehmen erfasst wurden." URL: http://privacy.microsoft.com/de¬de/default.aspx. In der vollständigen Online-Datenschutzerklärung macht Microsoft hinsichtlich der gemeinsamen Verwendung von Daten mit Werbepartnern auf Folgendes aufmerksam: „We also deliver advertisements and provide website analytics tools on non-Microsoft sites and services, and we may collect information about page views on these third party sites as well." (Wie schalten auch Werbeanzeigen und stellen Website-Analysewerkzeuge auf anderen Sites und für andere Dienste als von Microsoft bereit. Außerdem können wir Informationen darüber erheben, wie oft die Sites Dritter angezeigt wurden.) URL: http://privacy.microsoft.com/en-us/fullnotice.aspx. Google weist in seiner Datenschutzerklärung auf Folgendes hin: „Wir können die über Sie erhobenen personenbezogenen Daten mit Daten von anderen Google-Diensten oder anderen Unternehmen kombinieren, um das Angebot für unsere Nutzer zu verbessern, z. B. durch individuell auf Sie zugeschnittene Inhalte." URL: http://www.google.de/privacy.html. Yahoo! weist in seiner Datenschutzerklärung auf Folgendes hin: „Yahoo! may combine information about you that we have with information we obtain from business partners or other companies." (Yahoo! kann die Informationen über Sie mit Informationen kombinieren, die wir von Geschäftspartnern oder anderen Unternehmen erhalten.) URL: http://info.yahoo.com/privacy/us/yahoo/details.html

lung des (Such-) Dienstes nicht notwendig, wäre für eine rechtmäßige Verarbeitung die Einwilligung des Benutzers erforderlich, die ohne Zwang und in Kenntnis der Sachlage gegeben wurde.

6. VERPFLICHTUNG ZUR INFORMATION DER BETROFFENEN PERSON

Die meisten Internet-Benutzer wissen nicht, dass große Datenmengen über ihr Suchverhalten verarbeitet werden und für welche Zwecke diese Daten genutzt werden. Wenn sie sich dieser Verarbeitung nicht bewusst sind, können sie auch keine Entscheidungen in Kenntnis der Sachlage treffen.

Die Verpflichtung zur Information der betroffenen Personen über die Verarbeitung ihrer Daten gehört zu den fundamentalen Grundsätzen der Datenschutzrichtlinie. Artikel 10 regelt die Bereitstellung dieser Informationen, wenn die Daten direkt bei der betroffenen Person erhoben wurden. Die für die Verarbeitung Verantwortlichen sind verpflichtet, der betroffenen Person die folgenden Informationen mitzuteilen:

- Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters;

- Zweckbestimmungen der Verarbeitung, für die die Daten bestimmt sind;

- weitere Informationen, beispielsweise betreffend

  - die Empfänger oder Kategorien der Empfänger der Daten;

  - die Frage, ob die Beantwortung der Fragen obligatorisch oder freiwillig ist, sowie mögliche Folgen einer unterlassenen Beantwortung;

  - das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten.

In ihrer Rolle als Verantwortliche für die Verarbeitung von Benutzerdaten sollten die Suchmaschinenbetreiber gegenüber den Benutzern klarstellen, welche Informationen über sie erfasst werden und für welche Zwecke diese bestimmt sind. Bei der Erhebung von personenbezogenen Daten sollte deren Verwendung allgemein beschrieben werden, auch wenn an anderer Stelle eine detailliertere Beschreibung aufgeführt ist. Ebenso sollten die Benutzer über Software informiert werden, z. B. über Cookies, die auf ihrem Computer beim Zugriff auf eine Website gesetzt werden, und wie diese abgelehnt oder gelöscht werden können. Die

Arbeitsgruppe hält diese Angaben im Falle von Suchmaschinen für notwendig, damit eine Verarbeitung nach Treu und Glauben gewährleistet werden kann.

In den Antworten der Suchmaschinenbetreiber auf den Fragebogen der Arbeitsgruppe finden sich bedeutende Unterschiede. Einige Suchmaschinen erfüllen die Auflagen der Richtlinie. Sie bieten sowohl auf ihrer Startseite als auch auf den bei einem Suchvorgang generierten Seiten Links zu ihren Datenschutzerklärungen und informieren über Cookies. Bei anderen Suchmaschinen gestaltet sich die Suche nach den Datenschutzerklärungen sehr schwierig. Die Benutzer müssen in der Lage sein, auf die Datenschutzerklärungen einfach zuzugreifen, bevor sie – unter anderem von der Startseite der Suchmaschine – einen Suchvorgang durchführen.

Nach den Empfehlungen der Arbeitsgruppe sollten die vollständigen Datenschutzerklärungen so umfassend und detailliert wie möglich sein und die in den Datenschutzgesetzen enthaltenen fundamentalen Grundsätze erwähnen.

Die Arbeitsgruppe weist darauf hin, dass viele Datenschutzerklärungen gewisse Mängel in Bezug auf die Auskunfts- und Löschungsrechte aufweisen, die der betroffenen Person gemäß Artikel 12, 13 und 14 der Datenschutzrichtlinie zustehen. Diese Rechte gehören zu den grundlegenden Elementen des Schutzes der Privatsphäre von Personen.

7. RECHTE DER BETROFFENEN PERSON

Die Suchmaschinen sollten die Auskunfts-, Berichtigungs- und Löschungsrechte der betroffenen Personen bezüglich sie betreffender Daten beachten. Diese Rechte gelten vor allem für die von den Suchmaschinen gespeicherten Daten von authentifizierten Benutzern, einschließlich Personenprofile. Diese Rechte gelten aber auch für nicht registrierte Benutzer, die über die Möglichkeit verfügen sollten, ihre Identität gegenüber dem Suchmaschinenbetreiber nachzuweisen, etwa durch Registrieren für den Zugriff auf künftige Daten und/oder mit einer Erklärung von ihrem Zugangsanbieter über die Verwendung einer bestimmten IP-Adresse in der Vergangenheit, über die Auskunft verlangt wird. Bei Inhaltsdaten liegt die Hauptverantwortung im Rahmen der europäischen Datenschutzgesetze generell nicht bei den Suchmaschinenbetreibern.

Die Arbeitsgruppe hat im Jahr 2000 in ihrem Arbeitspapier „Privatsphäre im Internet“[25] bereits folgende Erläuterungen abgegeben: *„Das „Personalisieren“ von Datenprofilen setzt die vorherige Einwilligung bei Kenntnis aller Details der*

[25] WP 37, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37de.pdf

betroffenen Personen voraus. Sie müssen das Recht haben, ihre Zustimmung jederzeit und mit sofortiger Wirkung zu entziehen. Die Nutzer müssen jederzeit Gelegenheit haben, ihre Datenprofile zu überprüfen. Sie müssen auch das Recht haben, die gespeicherten Daten zu berichtigen oder zu löschen."

Im konkreten Fall der Anwendung auf Suchmaschinen müssen die Benutzer das Recht haben, auf alle über sie gespeicherten personenbezogenen Daten gemäß Artikel 12 der Datenschutzrichtlinie (95/46/EG) zuzugreifen. Dies gilt auch für ihre bisherigen Suchvorgänge, aus anderen Quellen erfasste Daten und Daten, die ihr Verhalten oder ihre Herkunft offenbaren. Die Artikel-29-Arbeitsgruppe hält es für überaus wichtig, dass die Suchmaschinenbetreiber die notwendigen Mittel für die Ausübung dieser Rechte bereitstellen, z. B. ein webbasiertes Instrument, das registrierten Benutzern direkten Online-Zugriff auf ihre personenbezogenen Daten mit der Möglichkeit bietet, bestimmte Verarbeitungszwecke abzulehnen.

Zweitens gilt das Recht auf Berichtigung oder Löschung von Informationen auch für spezifische Daten im Cache-Speicher der Suchmaschinenbetreiber, sobald diese Daten nicht mehr mit den tatsächlichen Inhalten übereinstimmen, die im Internet von den für die Verarbeitung Verantwortlichen der Website(s) veröffentlicht werden.[26] In einer derartigen Situation müssen die Suchmaschinenbetreiber bei Eingang eines Antrags von einer betroffenen Person sofort reagieren und unvollständige oder veraltete Informationen entfernen oder berichtigen. Der Cache-Speicher kann durch einen automatischen, sofortigen Neubesuch der ursprünglichen Veröffentlichung aktualisiert werden. Die Suchmaschinenbetreiber sollten den Benutzern die Möglichkeit bieten, die kostenlose Entfernung derartiger Inhalte aus ihrem Cache-Speicher anzufordern.

8. SCHLUSSFOLGERUNGEN

Das Internet wurde als ein offenes globales Netzwerk für den Informationsaustausch konzipiert. Es ist jedoch notwendig, ein Gleichgewicht zwischen der Offenheit des Internet und dem Schutz der personenbezogenen Daten von Internet-Benutzern zu finden. Dieses Gleichgewicht kann durch Differenzierung zwischen den zwei verschiedenen Hauptrollen von Suchmaschinenbetreibern hergestellt werden. In ihrer ersten Rolle als Verantwortliche für die Verarbeitung von Benutzerdaten (z. B. die IP-Adressen, die sie von Benutzern und ihrer individuellen Suchhistorie sammeln) sind sie im Rahmen der Datenschutzrichtlinie voll verantwortlich zu machen. In ihrer zweiten Rolle als Anbieter von Inhaltsdaten (z. B. den Daten im Index) liegt die Hauptverantwortung für die von ihnen verarbeiteten Daten im Rahmen der europäischen Datenschutzgesetze generell nicht

[26] Die Arbeitsgruppe schlägt vor, dass Herausgeber von Webseiten Maßnahmen entwickeln, um Suchmaschinen automatisch über eingegangene Anträge auf Löschung personenbezogener Daten zu informieren.

bei den Suchmaschinenbetreibern. Ausnahmen sind die Verfügbarkeit eines „Langzeit-Caches“ und Mehrwert schaffende Vorgänge für personenbezogene Daten (z. B. Suchmaschinen, die Profile von natürlichen Personen erstellen). Bei der Bereitstellung derartiger Dienste tragen die Suchmaschinen im Rahmen der Datenschutzrichtlinie die volle Verantwortung und müssen alle einschlägigen Bestimmungen einhalten.

Gemäß Artikel 4 der Datenschutzrichtlinie gelten dessen Bestimmungen für einen für die Verarbeitung Verantwortlichen, der eine Niederlassung im Hoheitsgebiet von mindestens einem an der Verarbeitung personenbezogener Daten beteiligten Mitgliedstaat besitzt. Die Bestimmungen der Richtlinie können aber auch auf nicht im gemeinschaftlichen Hoheitsgebiet niedergelassene Suchmaschinenbetreiber anwendbar sein, wenn diese zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreifen, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind.

Ausgehend von den obigen Überlegungen und unter Berücksichtigung der gegenwärtigen Vorgehensweise der Suchmaschinen können die folgenden Schlussfolgerungen gezogen werden:

Anwendbarkeit der EG-Richtlinien

1. **Die Datenschutzrichtlinie (95/46/EG) ist grundsätzlich auf die Verarbeitung von personenbezogenen Daten durch Suchmaschinenbetreiber anwendbar, auch wenn sich deren Hauptsitz außerhalb des EWR befindet.**

2. **Nicht im EWR ansässige Suchmaschinenbetreiber sollten ihre Benutzer darüber informieren, welche Bedingungen – Vorhandensein einer Niederlassung oder verwendete technische Mittel – sie zur Einhaltung der Datenschutzrichtlinie verpflichten.**

3. **Die Richtlinie über die Vorratsspeicherung von Daten (2006/24/EG) ist nicht auf Internet-Suchmaschinen anwendbar.**

Pflichten der Suchmaschinenbetreiber

4. **Personenbezogene Daten dürfen von den Suchmaschinenbetreibern nur für rechtmäßige Zwecke verarbeitet werden, und die Datenmenge muss für die verschiedenen zu erfüllenden Zwecke erheblich sein und darf nicht darüber hinausgehen.**

5. **Die Suchmaschinenbetreiber müssen personenbezogene Daten löschen oder (unumkehrbar und wirksam) anonymisieren, sobald sie für den Zweck, für den sie erhoben wurden, nicht mehr notwendig sind. Die Ar-**

beitsgruppe fordert die Suchmaschinenbetreiber zur Entwicklung geeigneter Anonymisierungssysteme auf.

6. **Die Speicherungsfristen sollten auf ein Minimum reduziert werden und in einem angemessenen Verhältnis zum jeweiligen von den Suchmaschinenbetreibern angeführten Zweck stehen. Angesichts der bisher abgegebenen Stellungnahmen der Suchmaschinenbetreiber zu den möglichen Zwecken für die Erhebung personenbezogener Daten sieht die Arbeitsgruppe keine Grundlage für eine Speicherungsfrist von mehr als sechs Monaten. In den einzelstaatlichen Rechtsvorschriften kann die Löschung von personenbezogenen Daten jedoch bereits zu einem früheren Zeitpunkt vorgeschrieben sein. Sofern die Suchmaschinenbetreiber personenbezogene Daten länger als sechs Monate speichern, müssen sie umfassend nachweisen, dass dies für den Dienst zwingend notwendig ist. Auf jeden Fall sollte die Information über die von den Suchmaschinenbetreibern festgelegten Speicherungsfristen auf ihrer Startseite einfach zugänglich sein.**

7. **Auch wenn die Erhebung einiger personenbezogener Daten über die Benutzer der Dienste durch Suchmaschinenbetreiber unvermeidlich ist, wie z. B. die Erhebung der IP-Adresse aufgrund des normalen HTTP-Verkehrs, ist die Erhebung zusätzlicher personenbezogener Daten von einzelnen Benutzern nicht notwendig, um Suchergebnisse liefern und Werbeanzeigen schalten zu können.**

8. **Wenn die Suchmaschinenbetreiber Cookies verwenden, sollte deren Lebensdauer nicht länger als nachweisbar notwendig sein. Ähnlich wie Web-Cookies sollten Flash-Cookies nur installiert werden, wenn transparente Informationen über ihre Zweckbestimmung und die Vorgehensweise für den Zugriff auf diese Information sowie ihre Bearbeitung und Löschung mitgeteilt werden.**

9. **Die Suchmaschinenbetreiber müssen den Benutzern klare und verständliche Informationen über ihre Identität, ihre Niederlassung und die Daten geben, die sie zu erheben, zu speichern oder zu übermitteln beabsichtigen, sowie über deren Zweckbestimmung.**[27]

10. **Die Anreicherung von Benutzerprofilen mit Daten, die nicht von den Benutzern selbst bereitgestellt werden, darf nur mit Einwilligung der Benutzer erfolgen.**

---

[27] Die Arbeitsgruppe empfiehlt ein mehrere Ebenen umfassendes Modell für die Datenschutzerklärung, so wie es in der Stellungnahme zu einheitlicheren Bestimmungen über Informationspflichten beschrieben wird (WP 100, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_de.pdf).

11. Wenn die Suchmaschinenbetreiber Mittel zur Speicherung der individuellen Suchhistorie bereitstellen, sollten sie sich vergewissern, dass die Einwilligung des Benutzers vorliegt.

12. Die Suchmaschinenbetreiber sollten die Nichtbeteiligungsklauseln von Website-Herausgebern respektieren, die festlegen, dass die Website nicht durchsucht und indexiert oder in den Cache-Speicher der Suchmaschinen aufgenommen werden soll.

13. Wenn die Suchmaschinenbetreiber einen Cache-Speicher bereitstellen, in dem personenbezogene Daten länger als in der ursprünglichen Veröffentlichung verfügbar gemacht werden, müssen sie das Recht der betroffenen Personen respektieren, über den Zweck hinausgehende und unrichtige Daten aus dem Cache-Speicher entfernen zu lassen.

14. Suchmaschinenbetreiber, die sich auf Mehrwert schaffende Vorgänge spezialisieren, wie z. B. Profilbildungsdienste für natürliche Personen (so genannte „Menschen-Suchmaschinen") und Gesichtserkennungssoftware für Bilder, müssen einen rechtmäßigen Grund für die Verarbeitung besitzen (z. B. die Einwilligung) und alle anderen Forderungen der Datenschutzrichtlinie erfüllen, wie etwa die Verpflichtung, die Qualität der Daten und die Verarbeitung nach Treu und Glauben zu gewährleisten.

<u>Rechte der Benutzer</u>

15. Benutzer von Suchmaschinendiensten besitzen das Recht, auf alle über sie gespeicherten personenbezogenen Daten einschließlich ihrer Profile und Suchhistorie zuzugreifen und diese, falls notwendiggemäß Artikel 12 der Datenschutzrichtlinie (95/46/EG) zu überprüfen und zu berichtigen.

16. Eine übergreifende Korrelation von Daten aus verschiedenen Diensten des Suchmaschinenbetreibers darf nur durchgeführt werden, wenn die Einwilligung des Benutzers für diesen speziellen Dienst vorliegt.

Brüssel, den 4. April 2008

Für die Datenschutzgruppe
Der Vorsitzende
Alex TÜRK

ANHANG 1

BEISPIELE FÜR DIE VON SUCHMASCHINEN VERARBEITETEN DATEN UND TERMINOLOGIE

Abfrageprotokolle	
Suchanfrage	Die in den Suchmaschinendienst eingegebene Suchanfrage, die gewöhnlich in Suchmaschinenprotokollen als URL der aufgrund der Suchanfrage angebotenen Seite gespeichert wird.
IP-Adresse	Die Internet-Protokolladresse des Computers für jede vom Benutzer eingegebene Anfrage.
Datum und Uhrzeit	Datum und Uhrzeit einer bestimmten Suchanfrage.
Cookie	Cookie(s) und/oder ähnliche auf dem Computer des Benutzers gespeicherte Objekte, einschließlich aller Cookie-Parameter, z. B. Wert und Verfallsdatum. Auf dem Server der Suchmaschine sind dies alle Daten, die sich auf das Cookie beziehen, z. B. die folgenden Informationen: „cookie/device X has been placed on computer with IP address Y, on date and time Z“ (Cookie/Objekt X wurde auf dem Computer mit der IP-Adresse Y am Datum und zur Uhrzeit Z gespeichert).
Flash-Cookie	Auch als „Local Shared Object“ bezeichnet. Ein Cookie, das mittels Flash-Technologie installiert wird. Im Gegensatz zu herkömmlichen Web-Cookies kann es derzeit nicht einfach über die Browser-Einstellungen gelöscht werden.
Referring-URL	Die URL der Website, auf der die Suchanfrage eingegeben wurde, eventuell eine URL Dritter.
Einstellungen	Mögliche benutzerspezifische Einstellungen in erweiterten Dienstumgebungen.
Browser	Einzelheiten zum Browser einschließlich des Typs und der Version.
Betriebssystem	Einzelheiten zum Betriebssystem.
Sprache	Spracheinstellungen des vom Benutzer verwendeten Browsers, aus denen sich die vom Benutzer bevorzugte Sprache ableiten lässt.
Angebotene Inhalte	
Links (Verknüpfungen)	Die Links, die einem bestimmten Benutzer aufgrund einer Anfrage zu einem bestimmten Zeitpunkt (Datum und Uhrzeit) angeboten wurden. Die Ergebnisse der Suchmaschine sind dynamisch. Damit die Ergebnisse im Detail ausgewertet werden können, muss der Suchmaschinenbetreiber Daten über die spezifischen Links und die Reihenfolge speichern, in der die Daten zu einem bestimmten Zeitpunkt (Datum und Uhrzeit) aufgrund einer spezifischen Benutzeranfrage angezeigt wurden.

Werbung	Die aufgrund einer bestimmten Suchanfrage angezeigte Werbung.
Benutzernavigation	Klicks durch den Benutzer auf die organischen Ergebnisse und Werbeanzeigen der Suchergebnisseite(n). Dies umfasst den Rang der spezifischen Ergebnisse, die vom Benutzer weiterverfolgt wurden (Link Nr. 1 wurde zuerst verfolgt, daraufhin kehrte der Benutzer zurück und folgte dem Link Nr. 8).
Operative Daten	Aufgrund des operativen Wertes und der Verwendung einiger der oben beschriebenen Daten (z. B. Betrugserkennung, Sicherheit/Integrität des Dienstes und Erstellung von Benutzerprofilen) werden diese Daten von den Suchmaschinen auf verschiedene Weise gekennzeichnet und analysiert. Beispielsweise kann eine bestimmte IP-Adresse als mögliche Quelle einer Anfrage oder von Klick-Spam gekennzeichnet werden; ein Klick auf eine Werbeanzeige kann als Betrug oder eine Anfrage als Verweis auf Informationsquellen zu einem bestimmten Thema gekennzeichnet werden.
Daten über registrierte Benutzer	Ein Suchmaschinenbetreiber kann den Benutzern anbieten, sich für die Nutzung von erweiterten Diensten registrieren zu lassen. Der Betreiber verarbeitet typischerweise Benutzerkontodaten, wie beispielsweise die Anmelde- und Kennwortdaten des Benutzers, eine Adresse für elektronische Post und andere vom Benutzer angegebene, personenbezogene Daten wie Interessen, Vorlieben, Alter und Geschlecht.
Daten anderer Dienste / Quellen	Die meisten Suchmaschinenbetreiber bieten zusätzliche Dienste wie elektronische Post, Desktop-Suche und Werbung auf Websites sowie für die Dienste Dritter an. Diese Dienste erzeugen Benutzerdaten, die korreliert und verwendet werden können, um das vorhandene Wissen über die Benutzer der Suchmaschine zu erweitern. Die Benutzerdaten und möglichen Profile können auch mit Daten aus anderen Quellen angereichert werden, z. B. mit Geolokationsdaten von IP-Adressen und demografischen Daten.

ANHANG 2

Fragebogen für Suchmaschinenbetreiber zur Datenschutzerklärung

1. Speichern Sie Daten über die individuelle Nutzung Ihrer Suchdienste?

2. Welche Art von Informationen speichern/archivieren Sie im Zusammenhang mit Ihren Suchdiensten? (z. B. Server-Protokolle, Schlüsselwörter, Suchergebnisse, IP-Adressen, Cookies, Klickdaten, Momentaufnahmen von Websites (Caches) usw.)

3. Fordern Sie die Einwilligung (freie Willenserklärung) des Benutzers bei der Speicherung der Daten an, die Sie in Ihrer Antwort auf Frage 2 genannt haben? Falls ja, wie fordern Sie sie an? Falls nein, auf welcher Rechtsgrundlage begründen Sie die Speicherung dieser Daten?

4. Erstellen Sie Profile über das Benutzerverhalten auf Basis der Daten, die Sie in Ihrer Antwort auf Frage 2 angegeben haben? Falls ja, für welche Zwecke? Welche Daten verarbeiten Sie? Unter welcher Kennung (z. B. IP-Adresse, Benutzerkennung, Cookie-ID) speichern Sie Profile? Fordern Sie die Einwilligung des Benutzers an?

5. Falls Sie zusätzlich zu den Suchdiensten andere personalisierte Dienste anbieten: Nutzen Sie die im Rahmen Ihrer Suchdienste erhobenen Daten gemeinsam mit diesen anderen Diensten und/oder umgekehrt? Falls ja, geben Sie bitte an, welche Daten dies betrifft.

6. Wie lange speichern Sie die Daten, die Sie in Ihrer Antwort auf Frage 2 angegeben haben, und für welche Zwecke?

7. Welche Kriterien sind bei der Festlegung der Speicherungsfrist für Sie maßgeblich?

8. Falls Sie Daten über einen befristeten Zeitraum speichern: Was tun Sie nach Ablauf dieser Frist, und welche diesbezüglichen Verfahren sind vorhanden?

9. Anonymisieren Sie Daten? Falls ja: Wie anonymisieren Sie die Daten? Ist die Anonymisierung unumkehrbar? Welche Informationen sind in den anonymisierten Daten immer noch enthalten?

10. Bestehen Zugriffsmöglichkeiten auf die Daten, z. B. für Personal, oder werden sie ohne menschliche Eingriffe verarbeitet?

11. Geben Sie Daten an Dritte weiter? In welchen Ländern? Geben Sie bitte für die folgenden Kategorien an, welche Arten von Daten Sie eventuell weitergeben und in welchen Ländern dies der Fall ist:

    – Werbetreibende

    – Werbepartner

    – Strafverfolgungsbehörden (Einhaltung rechtlicher Verpflichtungen zur Offenlegung der Daten, beispielsweise vor Gericht)

    – Sonstige (bitte angeben):

12. Wie informieren Sie die Benutzer über die Datenerhebung, Datenverarbeitung und Datenspeicherung? Geben Sie den Benutzern umfassende Informationen, z. B. über Cookies, Profilbildung und sonstige Werkzeuge, die die Aktivitäten auf der Website überwachen? Falls ja, fügen Sie bitte eine Kopie der Informationshinweise sowie eine Beschreibung ihrer Anordnung an.

13. Geben Sie den Benutzern die Möglichkeit, das Zugangsrecht und das Recht auf Berichtigung, Änderung, Löschung oder Sperrung der Daten auszuüben? Besteht die Möglichkeit, sich der Datenerhebung oder -speicherung vollständig zu entziehen („Opt-out“), so dass keine personenbezogenen Daten erhoben werden und der Benutzer keinerlei Spuren auf einem relevanten Speichersystem hinterlässt? Ist die Ausübung dieser Rechte mit Kosten verbunden?

14. Wenden Sie Sicherheitsmaßnahmen auf die Datenspeicherung an? Welche?

15. Haben Sie sich mit einer nationalen Datenschutzbehörde im EWR in Verbindung gesetzt? Falls ja, geben Sie bitte die Behörde an. Falls nein, geben Sie bitte die Gründe an, weshalb Sie dies bisher unterlassen haben.

Arbeitsdokument mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR) (WP 153)

Angenommen am 24. Juni 2008

EINFÜHRUNG

Die nachstehende Übersicht wurde von der Artikel-29-Datenschutzgruppe in der Absicht erstellt, Unternehmensgruppen, die Daten an ihre Mitglieder außerhalb der EU übermitteln, die Anwendung ihrer verbindlichen unternehmensinternen Datenschutzregelungen (Binding Corporate Rules – BCR) zu erleichtern:

– In der Übersicht ist aufgeführt, was in den BCR nach Maßgabe der Arbeitsdokumente WP 74[1] und WP 108[2] geregelt werden muss.

– Es wird genau angegeben, welche Bestimmungen in die BCR aufzunehmen sind und welche Angaben das Antragsformular für die Genehmigung der BCR enthalten muss (Arbeitsdokument WP 133[3]).

– Zum besseren Verständnis wird grundsätzlich auf die entsprechenden Textstellen in den Arbeitsdokumenten WP 74[4] und WP 108[5] verwiesen.

– Jeder Grundsatz wird gesondert erläutert bzw. kommentiert.

---

1 Arbeitsdokument WP 74: „Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer“, angenommen am 3. Juni 2003.
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_de.htm.

2 Arbeitsdokument WP 108: „Einführung eines Prüfungskatalogs für einen Antrag auf Genehmigung verbindlicher unternehmensinterner Vorschriften“, angenommen am 14. April 2005.
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_de.htm.

3 Arbeitsdokument WP 133: Empfehlung 1/2007 über das Antragsformular für die Genehmigung von verbindlichen unternehmensinternen Datenschutzregelungen zur Übermittlung personenbezogener Daten.
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_de.htm (nur EN).

4 Vgl. Fußnote 1.

5 Vgl. Fußnote 2.

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	Quelle	Bemerkungen
1 BINDUNG IM INNENVERHÄLTNIS				
1.1 Pflicht zur Einhaltung der BCR	JA	JA	WP 74 Ziff. 3.3.1 (Seiten 10–11) + WP 108 Ziff. 5.3 bis 5.9 (Seiten 5–6)	Die BCR müssen für alle Mitglieder der Unternehmensgruppe und für alle Beschäftigten eine klare Pflicht zur Einhaltung der BCR begründen.
1.2 Erläuterung, wie die Verbindlichkeit der BCR gegenüber den Mitgliedern der Unternehmensgruppe und den Beschäftigten garantiert wird	NEIN	JA	WP 74 Ziff. 3.3.1 (Seiten 10–11) + WP 108 Ziff. 5.3 bis 5.9 (Seiten 5–6)	In ihrem Antrag muss die Unternehmensgruppe erläutern, wie die Verbindlichkeit der BCR garantiert werden soll: i) im Verhältnis zwischen den Unternehmen/Unternehmensteilen der Gruppe durch: Vereinbarungen innerhalb der Gruppe Einseitige Erklärungen/Verpflichtungen Interne Regelungen Unternehmensgrundsätze oder Andere Maßnahmen ii) gegenüber den Beschäftigten durch: Individuelle Vereinbarung/Verpflichtung mit Sanktionen Klausel in Arbeitsverträgen mit Sanktionen Interne Unternehmensgrundsätze mit Sanktionen oder Tarifvertragliche Vereinbarungen mit Sanktionen
AUSSENVERHÄLTNIS				
1.3 Drittbegünstigung für Betroffene einschließlich der Möglichkeit der Beschwerde bei den zuständigen Datenschutzbehörden und der gerichtlichen Klage (wahlweise am Gerichtsstand des Datenexporteurs/der EU-Hauptniederlassung/des Unternehmens, das in der EU für den Datenschutz zuständig ist)	JA	JA	WP 74 Ziff. 3.3.2 (Seiten 11–13), Ziff. 5.5.1 (Seite 18) und Ziff. 5.6 (Seite 20) + WP 108 Ziff. 5.12 bis 5.14, Ziff. 5.16, Ziff. 5.20 (Seiten 6–7)	Die BCR müssen den betroffenen Personen als Drittbegünstigte Durchsetzungsrechte einräumen. Hierzu zählen gerichtliche Rechtsbehelfe bei Verstoß gegen garantierte Rechte und Schadenersatzansprüche (vgl. Artikel 22 und 23 der EU-Richtlinie).

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	Quelle	Bemerkungen
1.4 Das Unternehmen akzeptiert die Pflicht zur Leistung von Schadenersatz und zur Abhilfe bei Verstößen gegen die BCR.	JA	JA	WP 74 Ziff. 3.3.1, (Seite 11), Ziff. 5.5.1 (Seite 18), Ziff. 5.5.2 (Seite 19), Ziff. 5.6 (Seite 20) + WP 108 Ziff. 5.17 (Seite 7)	Die BCR müssen die EU-Hauptniederlassung oder das in der EU haftende Unternehmen verpflichten, die Haftung für Handlungen anderer Gruppenmitglieder außerhalb der EU, die an die BCR gebunden sind, zu übernehmen, Verstößen gegen die BCR abzuhelfen und Schadenersatz zu leisten. In den BCR muss auch festgelegt werden, dass im Falle eines Verstoßes gegen die BCR durch ein Mitglied der Unternehmensgruppe außerhalb der EU die Gerichte oder sonstige Behörden in der EU zuständig sind und der betroffenen Person gegenüber dem Mitglied, das die Haftung übernommen hat, dieselben Rechte und Abhilfen zustehen, als wenn der Verstoß von einem Mitglied innerhalb der EU begangen worden wäre. Ist es im Falle von Unternehmensgruppen mit einer besonderen Struktur nicht möglich, einem Mitglied der Gruppe die Haftung für außerhalb der EU begangene Verstöße gegen die BCR aufzuerlegen, können die Datenschutzbehörden im Einzelfall alternative Haftungslösungen akzeptieren, wenn der Antragsteller hinreichende Garantien bietet, dass die Rechte der Betroffenen durchsetzbar sind und dass diese bei der Durchsetzung ihrer Rechte nicht benachteiligt werden. Eine Möglichkeit bestünde in einer gesamtschuldnerischen Haftung der Datenimporteure und -exporteure wie in den EU-Standardvertragsklauseln 2001/497/EG vom 15. Juni 2001 oder in einer alternativen Haftungsregelung auf der Grundlage von Sorgfaltspflichten wie in den EU-Standardvertragsklauseln 2004/915/EG vom 27. Dezember 2004. Insbesondere bei der Weitergabe von Daten von für die Verarbeitung Verantwortlichen an Auftragsverarbeiter käme auch die Anwendung einer Haftungsregelung auf der Grundlage der Standardvertragsklauseln 2002/16/EG vom 27. Dezember 2001 in Frage.

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	Quelle	Bemerkungen
1.5 Das Unternehmen verfügt über ausreichende Mittel.	NEIN	JA	WP 74 Ziff. 5.5.2 (Seite 19) + WP 108 Ziff. 5.17 (Seite 7)	Dem Antrag muss eine Bestätigung beigefügt sein, wonach das Unternehmen, das die Haftung für Handlungen anderer Mitglieder außerhalb der EU, die an die BCR gebunden sind, übernommen hat, über ausreichende Mittel verfügt, um den Schaden zu ersetzen, der aus einer Verletzung der BCR entstanden ist.
1.6 Die Beweislast trägt das Unternehmen, nicht die betroffene Person.	JA	JA	WP 74 Ziff. 5.5.2 (Seiten 19–20) + WP 108 Ziff. 5.19 (Seite 7)	Aus den BCR muss hervorgehen, dass es dem Unternehmen, das die Haftung übernommen hat, obliegt nachzuweisen, dass der Verstoß gegen die BCR, mit dem die betroffene Person ihre Schadenersatzforderung begründet, nicht dem außerhalb der EU ansässigen Mitglied der Unternehmensgruppe zuzurechnen ist. Kann das Unternehmen, das die Haftung übernommen hat, nachweisen, dass die schadensbegründende Handlung nicht dem außerhalb der EU ansässigen Mitglied der Unternehmensgruppe zuzurechnen ist, so ist selbst von der Haftung befreit.
1.7 Die BCR sind für die betroffenen Personen leicht zugänglich. Gleiches gilt für Informationen über die Rechte der Betroffenen als Drittbegünstigte.	JA	NEIN	WP 74 Ziff. 5.7 (Seite 20)	Die BCR müssen für jede betroffene Person das Recht auf einfachen Zugang zu den BCR festschreiben. Auch die Klausel über die Drittbegünstigung sollte für alle betroffenen Personen, die Rechte als Drittbegünstigte in Anspruch nehmen können, leicht zugänglich sein. Beispielsweise könnte in den BCR festgehalten werden, dass die BCR im Internet oder im Intranet (wenn die Betroffenen Beschäftigte des Unternehmens sind) veröffentlicht werden.

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	Quelle	Bemerkungen
2 WIRKSAMKEIT				
2.1 Geeignete Schulungsprogramme	JA	JA	WP 74 Ziff. 5.1 (Seite 16) + WP 108 Ziff. 5.8–5.9 (Seite 6)	In den BCR muss festgelegt sein, dass die Mitarbeiter, die ständigen oder regelmäßigen Zugang zu Personaldaten haben, die solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln, eine geeignete Schulung zur Anwendung der BCR erhalten. Die Datenschutzbehörden, die den Antrag auf Genehmigung der BCR prüfen, können verlangen, dass das Schulungsprogramm, das im Antrag anzugeben ist, anhand von Beispielen oder anderweitig erläutert wird.
2.2 Beschwerdeverfahren	JA	JA	WP 74 Ziff. 5.3 (Seite 17) + WP 108 Ziff. 5.15 und 5.18 (Seite 7)	In den BCR ist ein internes Beschwerdeverfahren vorzusehen. Jede betroffene Person muss Beschwerde erheben können, wenn ein Mitglied der Unternehmensgruppe gegen die BCR verstößt. Mit den Beschwerden muss sich eine klar bezeichnete Beschwerdeabteilung oder Person befassen, die bei der Wahrnehmung dieser Aufgabe über ein entsprechendes Maß an Unabhängigkeit verfügt. Im Antrag ist anzugeben, wie die betroffenen Personen über die praktischen Aspekte des Beschwerdeverfahrens informiert werden, u. a.: – wo die Beschwerde einzureichen ist – in welcher Form – welche Fristen für die Bearbeitung der Beschwerde gelten – welche Folgen die Ablehnung der Beschwerde hat – welche Folgen die Anerkennung der Beschwerde hat – welche Rechtsbehelfe der betroffenen Person zur Verfügung stehen, wenn sie mit der Behandlung ihrer Beschwerde nicht zufrieden ist (Einlegung eines Rechtsbehelfs bei Gericht/der Datenschutzbehörde)

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	Quelle	Bemerkungen
2.3 BCR-Audit	JA	JA	WP 74 Ziff. 5.2 (Seiten 16–17) + WP 108 Ziff. 6 (Seiten 7–8)	In den BCR muss festgeschrieben sein, dass die Unternehmensgruppe verpflichtet ist, regelmäßig oder auf Antrag des Datenschutzbeauftragten (oder einer anderen zuständigen Stelle im Unternehmen) Datenschutzaudits durchzuführen (entweder durch interne oder durch externe akkreditierte Auditoren). Aus den BCR muss hervorgehen, dass sich das Auditprogramm auf alle Aspekte der BCR erstreckt und Verfahren vorsieht, mit denen sichergestellt wird, dass Abhilfemaßnahmen getroffen werden. In den BCR ist auch festzuhalten, dass das Ergebnis des Audits dem Datenschutzbeauftragten/der Datenschutzabteilung des Unternehmens sowie dem Aufsichtsrat der Muttergesellschaft mitgeteilt wird. Ferner ist in den BCR vorzusehen, dass den Datenschutzbehörden auf Antrag Zugang zu den Ergebnissen des Audits zu gewähren ist und dass sie berechtigt sind, bei Bedarf selbst einen Datenschutzaudit durchzuführen. Dem Antrag ist eine Beschreibung des Auditsystems beizufügen. Darin ist zum Beispiel anzugeben, – welche Abteilung innerhalb des Unternehmens über den Auditplan/das Auditprogramm entscheidet, – welche Abteilung das Audit durchführt, – wann das Audit durchgeführt wird (regelmäßig oder auf Antrag des Datenschutzbeauftragten), – Umfang des Audits (z. B. Anwendungen, IT-Systeme, Datenbanken, in denen Personaldaten verarbeitet werden, oder Weiterübermittlungen, Beschlüsse im Hinblick auf zwingende Erfordernisse nach nationalemRecht, die den BCR entgegenstehen, Überprüfung der Vertragsklauseln, auf deren Grundlage Daten an für die Verarbeitung Verantwortliche oder Auftragsverarbeiter außerhalb der Unternehmensgruppe übermittelt werden, Abhilfemaßnahmen usw.), – wer die Auditergebnisse erhält.

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	Quelle	Bemerkungen
2.4 Einrichtung eines Stabs von Datenschutzbeauftragten oder sonstigen befähigten Mitarbeitern, die Beschwerden bearbeiten, die Vorschriften überwachen und für deren Einhaltung sorgen	JA	NEIN	WP 74 Ziff. 5.1 (Seite 16) und 5.3 (Seite 17)	Selbstverpflichtung des Unternehmens, einen Mitarbeiterstab zu bilden (z. B. ein Netz von Datenschutzbeauftragten), der mit Unterstützung der Unternehmensspitze die Einhaltung der Vorschriften überwacht und gewährleistet. Kurze Beschreibung der Struktur, Aufgaben und Zuständigkeiten des Stabs der Mitarbeiter/Datenschutzbeauftragten o. ä., die die Einhaltung der BCR gewährleisten sollen. Z. B.: Der oberste Datenschutzbeauftragte berät die Unternehmensleitung, ist zuständig bei Untersuchungen der Datenschutzbehörden, berichtet jährlich über die Anwendung der BCR, sorgt auf Unternehmensebene für die Einhaltung der BCR. Die Datenschutzbeauftragten bearbeiten die Beschwerden der Betroffenen in ihrem Zuständigkeitsbereich, berichten dem obersten Datenschutzbeauftragten über größere Probleme beim Datenschutz und sorgen für die Einhaltung der Vorschriften auf lokaler Ebene.
3 KOOPERATIONSPFLICHT				
3.1 Pflicht zur Zusammenarbeit mit den Datenschutzbehörden	JA	JA	WP 74 Ziff. 5.4 (Seiten 17–18) + WP 108 Ziff. 5.21 (Seite 7)	Die BCR sollten alle Mitglieder der Unternehmensgruppe unmissverständlich dazu verpflichten, mit den Datenschutzbehörden zusammenzuarbeiten, deren Prüfungen zu dulden und ihren Mitteilungen, die die Anwendung der BCR betreffen, nachzukommen.

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	Quelle	Bemerkungen
4 BESCHREIBUNG DER DATENVERARBEITUNG UND DES DATENVERKEHRS				
4.1 Beschreibung der Übermittlungsvorgänge, die unter die BCR fallen	JA	JA	WP 74 Ziff. 4.1 Abs. 4 (Seite 15) + WP 108 Ziff. 7 (Seiten 8–9)	Die BCR müssen eine allgemeine Beschreibung der Übermittlungsvorgänge enthalten, damit die Datenschutzbehörden beurteilen können, ob die Datenverarbeitung in Drittländern einem angemessenen Schutzniveau genügt. Insbesondere sind anzugeben: i) Art der übermittelten Daten ii) Übermittlungs-/Verarbeitungszwecke iii) Datenimporteure/-exporteure innerhalb und außerhalb der EU Manche Datenschutzbehörden verlangen unter Umständen eine ausführliche Beschreibung des Datenverkehrs.
4.2 Erklärung zum Anwendungs- und Geltungsbereich der BCR (Art der Daten, Art der Betroffenen, Länder)	JA	JA	WP 108 Ziff. 7.1.1 und 7.2 (Seiten 8–9)	Aus den BCR sollte hervorgehen, ob sie anwendbar sind auf: i) alle personenbezogenen Daten, die innerhalb der Unternehmensgruppe aus der Europäischen Union in ein Drittland übermittelt werden, oder ii) jede Verarbeitung personenbezogener Daten, die innerhalb der Unternehmensgruppe erfolgt. In den BCR ist auch der materielle Anwendungsbereich anzugeben: z. B. personenbezogene Daten der Beschäftigten, Kunden, Lieferanten und anderer Dritter im Rahmen der regulären Geschäftstätigkeit des Unternehmens.

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	Quelle	Bemerkungen
5 SYSTEM FÜR DIE MELDUNG UND ERFASSUNG VON ÄNDERUNGEN				
5.1 Verfahren zur Aktualisierung der BCR	JA	JA	WP 74 Ziff. 4.2 (Seite 15) + WP 108 Ziff. 9 (Seite 10)	Die BCR können geändert werden *(z. B. zur Anpassung an eine Änderung der gesetzlichen Regelungen oder der Unternehmensstruktur)*, sie müssen jedoch eine Pflicht zur Meldung solcher Änderungen gegenüber allen Mitgliedern der Unternehmensgruppe und den Datenschutzbehörden vorsehen. Unter folgenden Voraussetzungen sind Aktualisierungen der BCR oder der Liste der Unternehmen, für die die BCR gelten, möglich, ohne eine neue Genehmigung beantragen zu müssen: i) Es wird eine Person benannt, die eine stets aktualisierte Liste der Gruppenmitglieder führt, Änderungen der BCR erfasst und den betroffenen Personen oder Datenschutzbehörden auf Anfrage diesbezügliche Auskünfte erteilt. ii) Einem neuen Mitglied der Unternehmensgruppe dürfen personenbezogene Daten erst dann übermittelt werden, wenn die BCR für dieses neue Mitglied gelten und die Einhaltung der Vorschriften gewährleistet ist. iii) Signifikante Änderungen der BCR oder der Mitgliederliste sollten den für die Genehmigung zuständigen Datenschutzbehörden jährlich mit einer kurzen Begründung der Änderungen gemeldet werden.

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	Quelle	Bemerkungen
6 DATENSCHUTZGARANTIEN				
6.1 Beschreibung der Datenschutzgrundsätze einschließlich der Vorschriften für die Datenübermittlung und die Weiterübermittlung aus der EU in Drittländer	JA	JA	WP 108 Ziff. 8 (Seite 9) + WP 74 Ziff. 3.1 letzter Abs. und Ziff. 3.2 (Seite 9)	In den BCR sollte erläutert werden, wie das Unternehmen die folgenden Grundsätze einhält: i) Transparenz, Fairness ii) Beschränkung der Zweckbestimmung iii) Datenqualität iv) Sicherheit – dies schließt die Pflicht ein, die Verwendung der Daten und die erforderlichen Sicherheitsvorkehrungen mit allen Unterauftragnehmern/Auftragsverarbeitern vertraglich zu regeln v) Recht auf Auskunft, Berichtigung und auf Widerspruch gegen die Verarbeitung vi) Beschränkung des Datentransfers und der Weiterübermittlung an Datenverarbeiter und für die Verarbeitung Verantwortliche, die nicht der Unternehmensgruppe angehören (die für die Verarbeitung Verantwortlichen, die Mitglieder der Unternehmensgruppe sind, können gruppenfremden Datenverarbeitern/für die Verarbeitung Verantwortlichen, die außerhalb der EU ansässig sind, unter der Bedingung Daten übermitteln, dass ein angemessener Schutz im Sinne der Artikel 16, 17, 25 und 26 der Richtlinie 95/46/EG gewährleistet ist)
6.2 Liste der Unternehmen, die an die BCR gebunden sind	NEIN	JA	WP 108 Ziff. 7.1.3 (Seite 9)	Siehe auch Ziff. 5.1 des vorliegenden Arbeitsdokuments WP 153: Pflicht zur Bestellung einer Kontaktperson in der Unternehmensgruppe, die die Liste der an die BCR gebundenen Unternehmen fortlaufend aktualisiert, und zur Unterrichtung der Datenschutzbehörden und der betroffenen Personen im Falle einer Änderung der Liste.

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	Quelle	Bemerkungen
6.3 Transparenzgebot in Fällen, in denen das einzelstaatliche Recht der Einhaltung der BCR durch die Unternehmensgruppe entgegensteht	JA	NEIN	WP 74 Ziff. 3.3.3 (Seiten 13–14)	Informationspflichten: Hat ein Unternehmen Anlass zu der Annahme, dass die es betreffenden Rechtsvorschriften es daran hindern, seinen Verpflichtungen im Rahmen der BCR nachzukommen, und dass diese Rechtsvorschriften die durch die BCR gebotenen Garantien wesentlich beeinträchtigen, muss es unverzüglich die Hauptniederlassung der Unternehmensgruppe in der EU oder das Unternehmen, das in der EU die Haftung für den Datenschutz übernommen hat, oder den zuständigen Datenschutzbeauftragten informieren (sofern dem nicht ein Verbot einer Vollstreckungsbehörde entgegensteht, z. B. zur Wahrung des Untersuchungsgeheimnisses in einer Strafsache). Im Falle einer Kollision zwischen nationalem Recht und den BCR beschließt die EU-Hauptniederlassung, das Unternehmen, das in der EU die Haftung für den Datenschutz übernommen hat, oder der zuständige Datenschutzbeauftragte nach Abwägung aller Argumente über das weitere Vorgehen und zieht im Zweifelsfall die zuständigen Datenschutzbehörden zu Rate.
6.4 Erklärung zum Verhältnis zwischen nationalen Rechtsvorschriften und BCR	NEIN (nicht obligatorisch, aber erwünscht)	NEIN (nicht obligatorisch, aber erwünscht)	o. A.	Eine Erklärung zum Verhältnis zwischen den BCR und dem einschlägigen anwendbaren Recht wird in WP 74 und WP 108 zwar nicht gefordert, wäre aber nützlich. So könnte in den BCR festgelegt werden, dass in Fällen, in denen das geltende Recht – z. B. EU-Recht – ein höheres Schutzniveau für personenbezogene Daten vorschreibt, dieses Recht den BCR vorgeht. Die Datenverarbeitung erfolgt in jedem Fall nach Maßgabe des anwendbaren Rechts im Sinne von Artikel 4 der Richtlinie 95/46/EG und der einschlägigen einzelstaatlichen Vorschriften.

Brüssel, den 24.6.2008

Für die Datenschutzgruppe
Der Vorsitzende Alex TÜRK

Arbeitsdokument „Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (BCR)“ (WP 154)

Angenommen am 24. Juni 2008

EINFÜHRUNG

Innerhalb einer Unternehmensgruppe dürfen personenbezogene Daten auf der Grundlage verbindlicher unternehmensinterner Datenschutzregelungen (Binding Corporate Rules – BCR) aus der EU in Drittländer übermittelt werden. Die Datenschutzgruppe hat in ihren Arbeitsdokumenten WP 74[1] und WP 108[2] Überlegungen zu den wesentlichen Bestandteilen solcher Regelungen angestellt.

Um Unternehmen bei der Ausarbeitung eigener BCR Hilfestellung zu leisten, hat die Gruppe den nachstehenden Rahmen ausgearbeitet, der zeigen soll, wie eine verbindliche unternehmensinterne Datenschutzregelung mit allen notwendigen Bestandteilen, die in den Arbeitsdokumenten WP 74[3] und WP 108[4] vorgestellt wurden, aussehen könnte.

1 Arbeitsdokument WP 74: „Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer“, angenommen am 3. Juni 2003.
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_de.htm

2 Arbeitsdokument WP 108: „Einführung eines Prüfungskatalogs für einen Antrag auf Genehmigung verbindlicher unternehmensinterner Vorschriften“, angenommen am 14. April 2005.
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_de.htm.

3 Vgl. Fußnote 1.

4 Vgl. Fußnote 2.

Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (Binding Corporate Rules – BCR)

HINWEIS

Es handelt sich hier nicht um ein Muster, sondern um einen Vorschlag, wie eine verbindliche unternehmensinterne Datenschutzregelung strukturiert werden und wie sie inhaltlich aussehen könnte.

Die BCR sollten auf die Struktur, Datenverarbeitung, Datenschutzpolitik und -verfahren der jeweiligen Unternehmensgruppe zugeschnitten sein. Die Datenschutzbehörden werden daher eine wortgetreue Wiedergabe des vorliegenden BCR-Rahmens nicht akzeptieren.

Die BCR sind Ausdruck der Datenschutzpolitik, die eine Unternehmensgruppe in Bezug auf die Übermittlung personenbezogener Daten aus der EU verfolgt. Sie können später zur Grundlage für die gesamte Verarbeitung aller Personaldaten in der Unternehmensgruppe werden.

Einleitung:

– Ausdrückliche Verpflichtung aller Mitglieder der Unternehmensgruppe und aller Beschäftigten zur Einhaltung der BCR

– Selbstverpflichtung der Unternehmensleitung, für die Einhaltung der BCR zu sorgen

– Ziele der BCR (angemessener Schutz der personenbezogenen Daten, die von der Unternehmensgruppe übermittelt und verarbeitet werden)

– Verweis auf die geltenden Datenschutzbestimmungen (EU-Richtlinien 95/46/EG und 2002/58/EG)

1 Anwendungs- und Geltungsbereich

Beschreibung des Anwendungs- und Geltungsbereichs der BCR, u. a.:

– Anwendung auf Übermittlungs- und Verarbeitungsvorgänge innerhalb der Unternehmensgruppe

– Geltungsbereich (nur Verarbeitungsvorgänge innerhalb der EU und Datenübermittlungen aus der EU in Drittländer oder sämtliche Verarbeitungs- und Übermittlungsvorgänge)

– Materieller Anwendungsbereich (z. R. Art der Datenverarbeitung: automatisiert/manuell, Art der Daten: Kunden/Mitarbeiter/Lieferanten)

Allgemeine Beschreibung des Datenverkehrs und der Verarbeitungszwecke einschließlich:

– Art der übermittelten Daten

– Übermittlungs-/Verarbeitungszwecke

– Datenimporteure/-exporteure innerhalb und außerhalb der EU[5]

2 Begriffsbestimmungen

Erläuterung der wichtigsten Begriffe:

– Personenbezogene Daten, sensible personenbezogene Daten, betroffene Person, für die Verarbeitung Verantwortlicher, Datenverarbeiter, Datenverarbeitung, Dritter, Datenschutzbehörden

– Erstellung eines Glossars mit anderen relevanten Begriffen wie Datenexporteur, Datenimporteur, EU-Hauptniederlassung/in der EU haftendes Unternehmen, Mitglied der Unternehmensgruppe[6], Datenschutzbeauftragter/für den Datenschutz zuständige Stelle

– Selbstverpflichtung zur Auslegung der BCR im Sinne der EU-Richtlinien 95/46/EG und 2002/58/EG

3 Zweckbindung

Beschreibung der Datenverarbeitungs- und übermittlungszwecke und Bestätigung folgender Grundsätze:

– Der Zweck der Verarbeitung und Übermittlung personenbezogener Daten muss eindeutig und rechtmäßig sein.

---

[5] Manche Datenschutzbehörden verlangen unter Umständen eine ausführlichere Beschreibung der Übermittlungs- und Verarbeitungsvorgänge.

[6] Ein Mitglied kann die Funktion eines für die Verarbeitung Verantwortlichen, eines Datenverarbeiters, eines Datenexporteurs oder -importeurs ausüben.

– Personenbezogene Daten dürfen nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden.

– Für sensible Daten werden zusätzliche Schutzvorkehrungen nach Maßgabe der EU-Richtlinie 95/46/EG getroffen.

4 Datenqualität und -verhältnismäßigkeit

In den BCR ist folgende Selbstverpflichtung aufzunehmen:

– Personenbezogene Daten müssen sachlich richtig sein und erforderlichenfalls auf den neuesten Stand gebracht werden.

– Personenbezogene Daten sollten den Zwecken entsprechen, für die sie übermittelt oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen.

– Personenbezogene Daten sollten nicht über einen längeren Zeitraum verarbeitet werden, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist.

5 Rechtsgrundlage für die Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten sollte auf folgender Grundlage erfolgen:

– Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben oder

– die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen; oder

– die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt; oder

– die Verarbeitung ist für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich; oder

– die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und die dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde; oder

– die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

6 Rechtsgrundlage für die Verarbeitung sensibler Daten

Sensible Daten dürfen nur unter folgenden Bedingungen verarbeitet werden:

– Die betroffene Person hat ausdrücklich in die Verarbeitung der genannten Daten eingewilligt, es sei denn, dieser Einwilligung steht ein gesetzliches Verbot entgegen; oder

– die Verarbeitung ist erforderlich, um den Rechten und Pflichten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund des einzelstaatlichen Rechts, das angemessene Garantien vorsieht, zulässig ist; oder

– die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten erforderlich, sofern die Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben; oder

– die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation, die keinen Erwerbszweck verfolgt, im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung nur auf die Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die Daten nicht ohne Einwilligung der betroffenen Personen an Dritte weitergegeben werden; oder

– die Verarbeitung bezieht sich auf Daten, die die betroffene Person offenkundig öffentlich gemacht hat; oder

– die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich; oder

– die Verarbeitung sensibler Daten ist zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich und erfolgt durch ärztliches Personal, das nach dem einzelstaatlichen Recht, einschließlich der von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen, dem Be-

rufsgeheimnis unterliegt, oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen.

7 Transparenz und Recht auf Information

Selbstverpflichtung, allen betroffenen Personen leichten Zugang zu den BCR zu gewähren

In den BCR sollte darüber hinaus beschrieben sein, wie die betroffenen Personen über die Übermittlung und Verarbeitung ihrer Personaldaten informiert werden.

Selbstverpflichtung zur Unterrichtung der betroffenen Personen vor Verarbeitung ihrer Daten über:

– die Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters

– die Zwecke der Verarbeitung, für die die Daten bestimmt sind,

– sowie über weitere Aspekte wie:

  i) die Datenempfänger oder Kategorien der Datenempfänger

  ii) das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten,

  sofern die Mitteilung dieser weiteren Aspekte unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig ist, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

Wurden die Daten nicht bei der betroffenen Person erhoben, besteht keine Pflicht zur Unterrichtung der betroffenen Person, wenn die Unterrichtung unmöglich ist, unverhältnismäßigen Aufwand erfordert oder die Speicherung oder Weitergabe durch Gesetz ausdrücklich vorgesehen ist.

8 Recht auf Auskunft, Berichtigung, Löschung oder Sperrung von Daten

In den BCR ist folgende Selbstverpflichtung aufzunehmen:

– Jede betroffene Person hat das Recht, frei und ungehindert in angemessenen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten eine Kopie al-

ler sie betreffenden Daten, die Gegenstand einer Verarbeitung sind, zu erhalten.

– Jede betroffene Person hat ein Recht auf Berichtigung, Löschung oder Sperrung von Daten, insbesondere wenn diese Daten unvollständig oder unrichtig sind.

– Jede betroffene Person hat das Recht, jederzeit aus zwingenden, berechtigten Gründen, die mit ihrer persönlichen Situation zusammenhängen, Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten einzulegen, es sei denn, die Verarbeitung dieser Daten ist gesetzlich vorgeschrieben. Ist der Widerspruch begründet, muss die Verarbeitung dieser Daten eingestellt werden.

– Jede betroffene Person hat das Recht, auf Antrag kostenfrei gegen eine Verarbeitung sie betreffender Daten für Zwecke der Direktwerbung Widerspruch einzulegen.

Erläuterung, wie die betroffenen Personen Auskünfte über ihre personenbezogenen Daten erlangen können

9 Automatisierte Einzelentscheidungen

Selbstverpflichtung, dass keine Entscheidung, die die betroffene Person erheblich beeinträchtigt, ausschließlich auf eine automatisierte Verarbeitung ihrer Daten gestützt wird, es sei denn,

– die Entscheidung ergeht im Rahmen des Abschlusses oder der Erfüllung eines Vertrags und dem Ersuchen der betroffenen Person auf Abschluss oder Erfüllung des Vertrags wurde stattgegeben oder die Wahrung ihrer berechtigten Interessen wird durch geeignete Maßnahmen – beispielsweise die Möglichkeit, ihren Standpunkt geltend zu machen – garantiert oder

– ist durch ein Gesetz zugelassen, das Garantien zur Wahrung der berechtigten Interessen der betroffenen Person festlegt.

10 Sicherheit und Vertraulichkeit

Selbstverpflichtung zur Anwendung geeigneter technischer und organisatorischer Sicherheitsmaßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und gegen jede andere Form der unrechtmäßigen Verarbeitung schützen

Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

Bei der Verarbeitung sensibler Daten sind erhöhte Sicherheitsmaßnahmen vorzusehen.

11 Verhältnis zu Datenverarbeitern, die der Unternehmensgruppe angehören

Erläuterung, wie personenbezogene Daten geschützt werden, wenn der Verarbeiter der Unternehmensgruppe angehört, insbesondere unter Beachtung folgender Grundsätze:

– Der für die Verarbeitung Verantwortliche muss einen Datenverarbeiter auswählen, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen eine ausreichende Gewähr bietet, und er muss für die Einhaltung dieser Maßnahmen sorgen.

– Der für die Verarbeitung Verantwortliche schließt mit dem Verarbeiter einen schriftlichen Vertrag nach Maßgabe des anwendbaren Rechts, in dem u. a. Folgendes festgelegt ist:

  i) Der Verarbeiter handelt nur auf Weisung des für die Verarbeitung Verantwortlichen.

  ii) Die Sicherheits- und Vertraulichkeitsbestimmungen gelten auch für den Verarbeiter.

12 Beschränkung des Datentransfers und der Weiterübermittlung an Datenverarbeiter und für die Verarbeitung Verantwortliche, die nicht der Unternehmensgruppe angehören

Erläuterung, wie der Datentransfer und die Weiterübermittlung außerhalb der Unternehmensgruppe beschränkt wird, und eine Selbstverpflichtung folgenden Inhalts:

– Mit externen Datenverarbeitern innerhalb der EU oder in einem Land mit einem von der EU-Kommission anerkannten angemessenen Datenschutzniveau wird schriftlich vereinbart, dass sie nur auf Weisung des für die Verarbeitung Verantwortlichen handeln und für die Durchführung geeigneter Maß-

nahmen zur Gewährleistung der Sicherheit und Vertraulichkeit der Datenverarbeitung verantwortlich sind.

– Bei der Übermittlung von Daten an externe für die Verarbeitung verantwortliche Personen außerhalb der EU sind die EU-Vorschriften für den grenzüberschreitenden Datenverkehr zu beachten (Artikel 25 und 26 der Richtlinie 95/46/EG: z. B. durch Bezugnahme auf die von der EU-Kommission gebilligten EU-Standardvertragsklauseln 2001/497/EG oder 2004/915/EG oder durch andere geeignete vertragliche Vereinbarungen nach Maßgabe der Artikel 25 und 26 der EU-Richtlinie).

– Bei der Übermittlung von Daten an externe Verarbeiter außerhalb der EU sind zusätzlich zu den Vorschriften für den grenzüberschreitenden Datenverkehr (Artikel 25 und 26 der Richtlinie 95/46/EG) die Vorschriften für Datenverarbeiter zu beachten (Artikel 16 und 17 der Richtlinie 95/46/EG).

13 Schulungsprogramm

Selbstverpflichtung zur Bereitstellung geeigneter BCR-Schulungsmaßnahmen für Mitarbeiter, die ständigen oder regelmäßigen Zugang zu Personaldaten haben, die solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln

14 Auditprogramm

Selbstverpflichtung, die Einhaltung der BCR innerhalb der Unternehmensgruppe einem Audit zu unterziehen, das u. a. durch folgende Merkmale gekennzeichnet ist:

– Das Auditprogramm erstreckt sich auf alle Aspekte der BCR und sieht Verfahren vor, mit denen sichergestellt wird, dass Abhilfemaßnahmen getroffen werden.

– Datenschutzaudits müssen regelmäßig (zeitliche Vorgabe) durch interne oder durch externe akkreditierte Auditoren oder auf Antrag des Datenschutzbeauftragten (oder einer anderen zuständigen Stelle im Unternehmen) durchgeführt werden.

– Die Auditergebnisse werden dem Datenschutzbeauftragten (oder einer anderen zuständigen Stelle im Unternehmen) und der Unternehmensleitung mitgeteilt.

– Die Datenschutzbehörden können eine Kopie dieser Audits anfordern.

– Im Auditplan ist vorzusehen, dass die Datenschutzbehörden bei Bedarf ein eigenes Datenschutzaudit durchführen können.

– Jedes Mitglied der Unternehmensgruppe muss solche Prüfungen der Datenschutzbehörden dulden und deren Mitteilungen, die die Anwendung der BCR betreffen, nachkommen.

15 Einhaltung der BCR und Überwachung

Selbstverpflichtung des Unternehmens, einen Mitarbeiterstab zu bilden (z. B. ein Netz von Datenschutzbeauftragten), der mit Unterstützung der Unternehmensspitze die Einhaltung der Vorschriften überwacht und gewährleistet

Kurze Beschreibung der Struktur, Aufgaben und Zuständigkeiten des Stabs der Mitarbeiter/Datenschutzbeauftragten o. ä., die die Einhaltung der BCR gewährleisten sollen. Z. B.: Der oberste Datenschutzbeauftragte berät die Unternehmensleitung, ist zuständig bei Untersuchungen der Datenschutzbehörden, berichtet jährlich über die Anwendung der BCR, sorgt auf Unternehmensebene für die Einhaltung der BCR. Die Datenschutzbeauftragten bearbeiten die Beschwerden der Betroffenen in ihrem Zuständigkeitsbereich, berichten dem obersten Datenschutzbeauftragten über größere Probleme beim Datenschutz und sorgen für die Einhaltung der Vorschriften auf lokaler Ebene.

16 Vorgehen bei einzelstaatlichen Vorschriften, die der Einhaltung der BCR entgegenstehen

Eindeutige Informationspflicht: Hat ein Unternehmen der Gruppe Anlass zu der Annahme, dass die es betreffenden Rechtsvorschriften es daran hindern, seinen Verpflichtungen im Rahmen der BCR nachzukommen, und dass diese Rechtsvorschriften die durch die BCR gebotenen Garantien wesentlich beeinträchtigen, muss es unverzüglich die Hauptniederlassung der Unternehmensgruppe in der EU oder das Unternehmen, das in der EU die Haftung für den Datenschutz übernommen hat, oder den zuständigen Datenschutzbeauftragten informieren (sofern dem nicht ein Verbot einer Vollstreckungsbehörde entgegensteht, z. B. zur Wahrung des Untersuchungsgeheimnisses in einer Strafsache).

Im Falle einer Kollision zwischen nationalem Recht und den BCR beschließt die EU-Hauptniederlassung, das Unternehmen, das in der EU die Haftung für den Datenschutz übernommen hat, oder der zuständige Datenschutzbeauftragte nach Abwägung aller Argumente über das weitere Vorgehen und zieht im Zweifelsfall die zuständigen Datenschutzbehörden zu Rate.

17 Interne Beschwerdeverfahren

Selbstverpflichtung zur Einführung eines Beschwerdeverfahrens, das folgenden Grundsätzen genügt:

– Jede betroffene Person muss Beschwerde mit der Begründung erheben können, dass ein Mitglied der Unternehmensgruppe gegen die BCR verstößt.

– Mit den Beschwerden muss sich eine klar bezeichnete Beschwerdeabteilung oder Person befassen, die bei der Wahrnehmung dieser Aufgabe über ein entsprechendes Maß an Unabhängigkeit verfügt.

18 Drittbegünstigung

Eine klare Aussage dahin gehend, dass die BCR den betroffenen Personen als Drittbegünstigte Durchsetzungsrechte einräumen. Hierzu zählen gerichtliche Rechtsbehelfe bei Verstoß gegen garantierte Rechte und Schadenersatzansprüche (vgl. Artikel 22 und 23 der EU-Richtlinie).

Erklärung dahin gehend, dass die betroffenen Personen ihre Beschwerde nach Wahl einlegen können:

– am Gerichtsstand des in der EU ansässigen Datenexporteurs,

– am Gerichtsstand der EU-Hauptniederlassung/des haftenden Unternehmens in der EU oder

– bei den zuständigen Datenschutzbehörden.

Selbstverpflichtung, dass die Klausel über die Drittbegünstigung für alle betroffenen Personen, die Rechte als Drittbegünstigte in Anspruch nehmen können, leicht zugänglich ist.

19 Haftung

Aufzunehmen ist eine Selbstverpflichtung folgenden Inhalts:

– Die EU-Hauptniederlassung oder das haftende Unternehmen in der EU[7] übernimmt die Haftung für Handlungen anderer Gruppenmitglieder außerhalb der

[7] Ist es im Falle von Unternehmensgruppen mit einer besonderen Struktur nicht möglich, einem Mitglied der Gruppe die Haftung für außerhalb der EU begangene Verstöße gegen die BCR aufzuerlegen, können die Datenschutzbehörden im Einzelfall alternative Haftungslösungen akzeptieren, wenn der Antragsteller hinreichende Garantien bietet, dass die Rechte der Betroffenen durchsetzbar sind und dass diese bei der Durchsetzung ihrer Rechte nicht benachteiligt werden. Eine Möglichkeit bestünde in einer gesamtschuldnerischen Haftung der Datenimporteure und -exporteure wie in den EU-Standardvertragsklauseln 2001/497/EG vom 15. Juni 2001 oder in einer alternativen Haftungsregelung auf der Grundlage von Sorgfaltspflichten wie in den EU-Standardvertragsklauseln 2004/915/EG vom 27. Dezember 2004. Insbesondere bei der Weitergabe von Daten von für die Verarbeitung Verantwortlichen an Auftragsverarbeiter käme auch die Anwendung einer Haftungsregelung auf der Grundlage der Standardvertragsklauseln 2002/16/EG vom 27. Dezember 2001 in Frage.

EU, ergreift die notwendigen Maßnahmen, um Verstößen gegen die BCR abzuhelfen, und leistet Ersatz für Schäden, die aus einem Verstoß gegen die BCR durch ein Mitglied der Unternehmensgruppe entstanden sind.

– Die Beweislast trägt entweder die EU-Hauptniederlassung oder das haftende Unternehmen in der EU, d. h. ihnen obliegt es nachzuweisen, dass der Verstoß gegen die BCR, mit dem die betroffene Person ihre Schadenersatzforderung begründet, nicht dem außerhalb der EU ansässigen Mitglied der Unternehmensgruppe zuzurechnen ist.

Die EU-Hauptniederlassung bzw. das haftende Unternehmen in der EU kann sich von der Haftung befreien, wenn es nachweist, dass die schadensbegründende Handlung nicht dem außerhalb der EU ansässigen Mitglied der Unternehmensgruppe zuzurechnen ist.

20 Gegenseitige Unterstützung und Zusammenarbeit mit den Datenschutzbehörden

Selbstverpflichtung dahin gehend, dass

– die Mitglieder der Unternehmensgruppe bei Anfragen oder Beschwerden einer betroffenen Person oder bei Untersuchungen oder Nachforschungen der Datenschutzbehörden zusammenarbeiten und einander unterstützen die Unternehmen den Mitteilungen der Datenschutzbehörden, die die Auslegung der BCR betreffen, nachkommen.

21 Aktualisierung der Vorschriften

Selbstverpflichtung zur Meldung signifikanter Änderungen der BCR oder der Mitgliederliste gegenüber allen Mitgliedern der Unternehmensgruppe und den Datenschutzbehörden, um Änderungen der gesetzlichen Regelungen oder der Unternehmensstruktur Rechnung zu tragen:

– Für manche Änderungen ist unter Umständen eine neue Genehmigung der Datenschutzbehörden erforderlich.

– Unter folgenden Voraussetzungen sind Aktualisierungen der BCR oder der Liste der Unternehmen, für die die BCR gelten, möglich, ohne eine neue Genehmigung beantragen zu müssen:

  i) Es wird eine Person benannt, die eine stets aktualisierte Liste der Gruppenmitglieder führt, Änderungen der BCR erfasst und den betroffenen

Personen oder Datenschutzbehörden auf Anfrage diesbezügliche Auskünfte erteilt.

ii) Einem neuen Mitglied der Unternehmensgruppe dürfen personenbezogene Daten erst dann übermittelt werden, wenn die BCR für dieses neue Mitglied gelten und die Einhaltung der Vorschriften gewährleistet ist.

iii) Signifikante Änderungen der BCR oder der Mitgliederliste sollten den für die Genehmigung zuständigen Datenschutzbehörden jährlich mit einer kurzen Begründung der Änderungen gemeldet werden.

Selbstverpflichtung dahin gehend, dass signifikante Änderungen der Vorschriften auch den betroffenen Personen mitgeteilt werden

22 Verhältnis zwischen einzelstaatlichem Recht und BCR

Erklärung, dass

– in Fällen, in denen das geltende Recht – z. B. EU-Recht – ein höheres Schutzniveau für personenbezogene Daten vorschreibt, dieses Recht den BCR vorgeht

– die Datenverarbeitung in jedem Fall nach Maßgabe des anwendbaren Rechts im Sinne von Artikel 4 der Richtlinie 95/46/EG und der einschlägigen einzelstaatlichen Vorschriften erfolgt

23 Schlussbestimmungen

– Zeitpunkt des Inkrafttretens

– Übergangszeit

Bei den Datenschutzbehörden einzureichende Unterlagen

1 Antragsformular WP 133

2 Unterlagen, die Aufschluss über die Einhaltung der BCR geben können, z. B.:

– Unterlagen, die Aufschluss über die Datenschutzpolitik u. a. gegenüber Kunden oder Mitarbeiter geben und aus denen hervorgeht, wie die Betrof-

fenen über den Schutz ihrer personenbezogenen Daten in der Unternehmensgruppe informiert werden

– Leitlinien für die Beschäftigten, die Zugang zu personenbezogenen Daten haben, um ihnen das Verständnis und die Anwendung der BCR zu erleichtern (z. B. Leitlinien für den Umgang mit Beschwerden, die Information der betroffenen Personen, für geeignete Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit der Datenverarbeitung)

– Datenschutzauditplan und -programm unter Angabe der zuständigen Personen (interne/externe akkreditierte Auditoren der Unternehmensgruppe)

– Beschreibung des Schulungsprogramms und/oder Beispiele

– Nachweis, dass das Unternehmen, von dem aus die Daten aus der EU in Drittländer übermittelt werden, und entweder die EU-Hauptniederlassung oder das in der EU haftende Unternehmen über ausreichende Mittel verfügen, um den Schaden zu ersetzen, der aus einer Verletzung der BCR entstanden ist

– Beschreibung des internen Beschwerdeverfahrens

– Liste der Unternehmen, die an die BCR gebunden sind

– Sicherheitspolitik in Bezug auf IT-Systeme, mit denen personenbezogene Daten aus der EU verarbeitet werden

– Zertifizierungsverfahren, mit dem gewährleistet ist, dass alle neuen IT-Anwendungen zur Verarbeitung von EU-Daten mit den BCR vereinbar sind

– Musterverträge für Datenverarbeiter (innerhalb oder außerhalb der Unternehmensgruppe), die EU-Daten verarbeiten

– Stellenbeschreibung des Datenschutzbeauftragten oder anderer Personen, die für den Datenschutz in der Unternehmensgruppe zuständig sind.

Brüssel, den 24.6.2008

Für die Datenschutzgruppe
Der Vorsitzende
Alex TÜRK

Stellungnahme 3/2008 zum Entwurf eines Internationalen Datenschutzstandards zum Welt-Anti-Doping-Code (WP 156)

Annahme am 1. August 2008

Die Arbeitsgruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten –

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,
gestützt auf Artikel 29 sowie Artikel 30 Absatz 1 Buchstabe a) und Absatz 3 der Richtlinie, sowie auf Artikel 15 Absatz 3 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002,
gestützt auf Artikel 255 des EG-Vertrags und auf die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission,
gestützt auf ihre Geschäftsordnung –

hat folgendes Dokument angenommen:

Einführung

Die Generaldirektion Bildung und Kultur (GD EAC) der Europäischen Kommission hat die Artikel-29-Datenschutzgruppe (Arbeitsgruppe) um eine Stellungnahme zum Entwurf eines von der Welt-Anti-Doping-Agentur (WADA) erarbeiteten Internationalen Datenschutzstandards ersucht.

Der Entwurf des Standards ist in Verbindung mit dem Welt-Anti-Doping-Code (der Code) der WADA, im Besonderen mit Artikel 14, zu sehen.

Nach dem Code sind die Athleten verpflichtet, den Anti-Doping-Organisationen regelmäßig bestimmte Daten zu übermitteln. Diese Daten werden anschließend zusammen mit anderen Daten (darunter auch sensible Daten) in der in Kanada geführten Datenbank ADAMS gespeichert.

Entsprechend den im Code festgelegten Verpflichtungen werden auch Daten verarbeitet, die ihre Betreuer – gemäß der Definition des Codes – sowie andere Personenkategorien betreffen. „Teilnehmer“ im Sinne des Codes sind sowohl die Athleten als auch ihre Betreuer.

Teil I – Einleitung, Bestimmungen des Codes und Definitionen

Punkt 2 – Bestimmungen des Codes

Obgleich sich die Stellungnahme der Arbeitsgruppe auf den Entwurf des Internationalen Standards, der der Arbeitsgruppe am 7. Juli 2008 vorgelegt wurde, und nicht auf den Welt-Anti-Doping-Code bezieht, weist die Arbeitsgruppe darauf hin, dass einige Bestimmungen des Codes (auf die im Entwurf des Standards Bezug genommen wird) Fragen über deren Vereinbarkeit mit europäischen Datenschutzstandards aufwerfen.

Alle an Anti-Doping-Aktivitäten beteiligten Personen haben ein Recht auf den Schutz ihrer Privatsphäre und ihrer personenbezogenen Daten und daher wird empfohlen, Artikel 14 des Codes wie folgt zu ändern: *„Die Unterzeichner stimmen den Grundsätzen der Behandlung der Ergebnisse der Dopingbekämpfung, der Transparenz und Rechenschaftspflicht gegenüber der Öffentlichkeit sowie der Achtung der Privatsphäre* ***aller Personen, auch*** *der eines Verstoßes gegen Anti-Doping-Bestimmungen Beschuldigten zu“.*

Artikel 14.2 – Offenlegung

Die Arbeitsgruppe erinnert daran, dass die Offenlegung und Weitergabe von Daten in den Geltungsbereich der Datenschutzvorschriften fällt. Die Arbeitsgruppe begrüßt, dass Entscheidungen über Fälle, in denen ein Athlet nicht gegen die Anti-Doping-Bestimmungen verstoßen hat, nur mit Zustimmung des Betroffenen offengelegt werden. Sie empfiehlt jedoch, den Wortlaut des Internationalen Standards so zu formulieren, dass für die Anti-Doping-Organisationen eindeutig klar wird, dass „angemessene Anstrengungen, um diese Zustimmung zu erhalten“, die tatsächliche Zustimmung zur Offenlegung nicht ersetzen können (siehe Artikel 14.2.3).

Die Arbeitsgruppe wirft außerdem die Frage auf, ob eine Datenverarbeitung, bei der Entscheidungen und sonstige Informationen, die Athleten oder andere „Personen“ betreffen, für mindestens ein Jahr auf der Website der Anti-Doping-Organisation (14.2.4 – siehe auch Teil II, Punkt 10, unten) eingestellt werden, noch verhältnismäßig ist. Die Arbeitsgruppe schlägt vor, die Bestimmungen des Standards auch auf diese „Personen“ anzuwenden, sofern es sich dabei nicht um die betroffenen Athleten oder deren Betreuer handelt. Es gibt keinen Grund, sie von dem in diesem Fall geltenden Schutz auszunehmen.

Artikel 14.5 (Datenbank ADAMS)

Abgesehen von dem kurzen Text in Artikel 14.4 des Codes enthält der Entwurf des Standards keine Präzisierung der Vorschriften, die für die Datenverarbeitung

im Zusammenhang mit der Datenbank ADAMS gelten. Der Entwurf des Standards bezieht sich ausschließlich auf die Anti-Doping-Organisationen. Die Einhaltung der Datenschutzbestimmungen bei der Dopingbekämpfung muss jedoch sowohl bei der Verarbeitung der Daten durch die Anti-Doping-Organisationen als auch bei der Nutzung der Datenbank ADAMS gewährleistet sein. Die Arbeitsgruppe stellt fest, dass diese Datenbank der Zuständigkeit der kanadischen Datenschutzbehörden unterliegt. Die Artikel-29-Arbeitsgruppe hält den knappen Verweis auf diese Datenbank im vorliegenden Standard jedoch nicht für ausreichend.

Die Arbeitsgruppe schlägt daher vor, dass entweder der Internationale Standard geändert wird und ausführlichere Angaben über die Datenbank ADAMS aufgenommen werden, oder dass die WADA Vorschriften für die Nutzung der Datenbank ADAMS festlegt. Zudem wird darauf hingewiesen, dass bei der Weitergabe von Daten durch die EU an Kanada sorgfältig darauf zu achten ist, dass dabei die EU-Rechtsvorschriften über angemessene Sicherheitsvorkehrungen für die Weiterübermittlung eingehalten werden.

Artikel 14.6

Eine Definition für den Begriff „Dritte“ liegt nicht vor.

Generell sollten die spezifischen Zwecke der gemäß dem Code durchgeführten Datenverarbeitung definiert werden. Der Hinweis, dass die Anti-Doping-Organisationen „im Zusammenhang mit Maßnahmen zur Dopingbekämpfung“ Daten verarbeiten, reicht allein nicht aus.

Punkt 3 – Begriffe und Definitionen

Teilnehmer

Die Arbeitsgruppe vertritt die Auffassung, dass der Begriff „Teilnehmer” – wie er im Code definiert wird – zu eng ausgelegt ist, um den Schutz aller Personen zu gewährleisten, deren personenbezogene Daten im Rahmen der Umsetzung des Codes verarbeitet werden können (siehe Anmerkungen oben zu Artikel 14.2.4 „Person“ und zu Artikel 14.6 „Dritte“). Die Arbeitsgruppe ist sich darüber im Klaren, dass nur Athleten und deren Betreuer zur Weitergabe personenbezogener Daten an die WADA verpflichtet sind, doch zur Vermeidung von Verwechslungen hält sie eine einheitliche Verwendung der Begriffe im Internationalen Standard und im Code für sinnvoll.

Drei neue Definitionen werden in Artikel 3.2. des Entwurfs des Standards eingeführt:

Personenbezogene Informationen

Die hier angegebene Definition schließt die Definition des Begriffs „personenbezogene Daten" in Artikel 2 Buchstabe a) der Datenschutzrichtlinie ein. Die Arbeitsgruppe stellt fest, dass der Entwurf des Standards außer in Artikel 9 (Gewährleistung der Sicherheit von personenbezogenen Informationen) keine zusätzlichen Garantien für den Schutz von Gesundheitsdaten und Strafverfolgungsdaten bietet, die im Rahmen der Anti-Doping-Maßnahmen verarbeitet werden.

Sensible personenbezogene Informationen

Die Definition der als sensibel angesehenen personenbezogenen Informationen steht im Einklang mit Artikel 8 der Richtlinie. Die Arbeitsgruppe verweist an dieser Stelle auf ihre Ausführungen zu Artikel 6 des Standards über die Verarbeitung solcher Daten (siehe unten).

Verarbeitung

Die Arbeitsgruppe hält diese Definition für ausreichend, auch wenn sie nicht im wörtlichen Sinne mit der Definition in Artikel 2 Buchstabe b) der Richtlinie übereinstimmt.

Teil II – Standards für den Umgang mit personenbezogenen Informationen

Punkt 4 – Verarbeitung personenbezogener Informationen nach Maßgabe des Internationalen Standards und des geltenden Rechts

Nach Ansicht der Arbeitsgruppe schließt die Bezeichnung „Vertreter Dritter" Auftragsverarbeiter im Sinne von Artikel 2 Buchstabe e) der Datenschutzrichtlinie ein. Die weiteren Anmerkungen zu diesem Begriff (siehe Punkt 9) basieren auf dieser Annahme. Der Anwendungsbereich dieses Begriffs sollte genau festgelegt werden.

Absatz 4.1

Die Arbeitsgruppe hält eine Änderung von Absatz 4.1 für sinnvoll, die klarstellt, dass Vertreter Dritter ebenfalls zur Einhaltung des Standards verpflichtet sind, auch wenn dieser über die nach nationalem Recht geltenden Standards hinausgeht.

Im Entwurf des Standards wird nicht zwischen den verschiedenen Personenkategorien (Athleten, Betreuer, Dritte), für die er gilt, unterschieden. Die Anwendung des Grundsatzes der Verhältnismäßigkeit wird jedoch von der Kategorie ab-

hängen, zu der die betroffene Person gehört (Welche Daten? Welche gespeicherten Daten?). Daher sollte der Entwurf des Standards entsprechend geändert werden.

Verarbeitung personenbezogener Daten, die im Hinblick auf den Zweck, für den sie erhoben wurden, relevant sind und nicht darüber hinausgehen

In Absatz 5.3 sollten die personenbezogenen Informationen oder die Kategorien von personenbezogenen Informationen erläutert werden, die unter Berücksichtigung der mit den Grundsätzen der Notwendigkeit und der Verhältnismäßigkeit verbundenen Anforderungen für die Zwecke benötigt werden, die unter Buchstaben a), b) und c) aufgeführt sind. Wie bereits erwähnt, wird die Anwendung dieser Grundsätze je nach Kategorie der Personen variieren, deren Daten verarbeitet werden (Athleten, Betreuer).

Nach Artikel 5.4 des Entwurfs des Standards müssen die verarbeiteten personenbezogenen Daten genau, vollständig und aktuell sein. Mit dem letzten Satz dieses Absatzes scheint diese Verpflichtung für die Anti-Doping-Organisationen jedoch abgeschwächt zu werden. Es hat sogar den Anschein, als ob die Verantwortung von dem für die Datenverarbeitung Verantwortlichen auf die betroffene Person abgewälzt werden soll.[1] Der Kommentar bestätigt diese Absicht im Wesentlichen. In diesem Zusammenhang hebt die Arbeitsgruppe hervor, dass gemäß Artikel 6 Buchstabe d) der Datenschutzrichtlinie alle erforderlichen Maßnahmen zu treffen sind, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, nicht zutreffende oder unvollständige Daten gelöscht oder berichtigt werden. Es ist Aufgabe des für die Datenverarbeitung Verantwortlichen, auf Antrag der betroffenen Personen die notwendigen Berichtigungen durchzuführen.

Punkt 6 – Verarbeitung personenbezogener Informationen mit Zustimmung

Nach Artikel 7 der Datenschutzrichtlinie muss für jede Datenverarbeitung eine gültige Rechtsgrundlage vorliegen. Bei der Verarbeitung von Gesundheitsdaten ist eine solche Rechtsgrundlage von grundlegender Bedeutung.

Artikel 6.1

In Artikel 6.1 des Entwurfs des Standards werden die Anti-Doping-Organisationen dazu aufgerufen, die Zustimmung der Athleten und der Mitglieder ihres Betreuungsteams einzuholen, um die Rechtmäßigkeit ihrer Datenverarbeitung zu gewährleisten. Nach Auffassung der Arbeitsgruppe erfüllt eine solche Zustim-

[1] „(…). Auch wenn dies nicht zwangsläufig bedeutet, dass die Anti-Doping-Organisationen die Richtigkeit aller von ihnen verarbeiteten personenbezogenen Daten überprüfen müssen, sind die Anti-Doping-Organisationen verpflichtet, sämtliche personenbezogenen Informationen so schnell wie möglich zu berichtigen oder zu ändern, von denen sie sicher wissen, dass sie falsch oder nicht zutreffend sind".

mung die in Artikel 2 Buchstabe h) der Datenschutzrichtlinie festgelegten Anforderungen nicht. Als Zustimmung wird gemäß dieser Definition *„jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden“* angesehen. Die Zustimmung zur Verarbeitung von Daten, die im Zusammenhang mit der Erfüllung der Verpflichtungen des Welt-Anti-Doping-Codes erhoben werden, erfolgt weder ohne Zwang noch in Kenntnis der Sachlage. Aufgrund der Sanktionen, die verhängt werden können, wenn sich ein Teilnehmer weigert, den Verpflichtungen des Codes (Übermittlung von Daten über Aufenthaltsort und Erreichbarkeit, medizinische Anti-Doping-Kontrollen) nachzukommen, gelangt die Arbeitsgruppe zu dem Schluss, dass die Zustimmung keineswegs ohne Zwang gegeben wird.[2] Ferner zieht die Arbeitsgruppe in Zweifel, ob die Zustimmung in Kenntnis der Sachlage erfolgt (siehe Punkt 7 unten).

Da Artikel 7 Buchstabe a) und Artikel 8 Buchstabe a) der Datenschutzrichtlinie nicht als Rechtsgrundlagen für die Datenverarbeitung in Frage kommen, muss dafür eine andere geeignete Rechtsgrundlage herangezogen werden. Die Arbeitsgruppe erinnert daran, dass die Verarbeitung von Daten über Verstöße nicht zulässig ist, selbst dann nicht, wenn die Zustimmung der betroffenen Person vorliegt und diese in Kenntnis der Sachlage erfolgt (Artikel 8 Absatz 2 der Datenschutzrichtlinie).

Die Arbeitsgruppe empfiehlt daher, dass die WADA prüft, welche anderen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten gemäß Artikel 7 und sensibler personenbezogener Daten gemäß Artikel 8 der Datenschutzrichtlinie in Frage kommen.

Mehrere internationale Übereinkommen zur Dopingbekämpfung, wie das Internationale Übereinkommen gegen Doping im Sport oder das Anti-Doping-Übereinkommen des Europarates, wären mögliche Rechtsgrundlagen für die Datenverarbeitung, sofern sich diese Übereinkommen auf eine bindende rechtliche Verpflichtung berufen, der Anti-Doping-Organisationen – gemäß der Umsetzung von Artikel 7 Buchstabe c) und Artikel 8 Absatz 4 der Datenschutzrichtlinie in nationales Recht – als die für die Verarbeitung Verantwortlichen unterliegen.

Artikel 6.2

Nach Artikel 6.2 des Entwurfs des Standards ist die Verarbeitung sensibler Daten, wie sie in Artikel 3.2 definiert werden, zulässig. Sensible Daten im Sinne der Da-

[2] In Artikel 6.3 des Entwurfs des Standards heißt es zum Beispiel, dass „die Teilnehmer von den Anti-Doping-Organisationen über die negativen Konsequenzen zu informieren sind, die ihre Weigerung, an Dopingkontrollen, einschließlich Tests, teilzunehmen, nach sich ziehen können“.

tenschutzrichtlinie sind personenbezogene Daten, die die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit oder das Sexualleben betreffen. Der Arbeitsgruppe erscheint es äußerst zweifelhaft, ob die Erheblichkeit der Verarbeitung von Daten aus einigen dieser Kategorien gewährleistet ist, insbesondere, wenn eine Aufnahme dieser Daten in die Datenbank ADAMS beabsichtigt ist. Daher fordert die Arbeitsgruppe die WADA auf, ausführlichere Informationen vorzulegen oder die Erheblichkeit einer möglichen Verarbeitung solcher Daten nochmals zu prüfen und in Artikel 6.2 die maßgeblichen Daten aufzuführen, die in diesem Rahmen verarbeitet werden sollen. Die Definition in Artikel 3.2 schließt zudem genetische Merkmale ein. Die Arbeitsgruppe stellt die Rechtmäßigkeit und die Notwendigkeit der Verarbeitung derartiger Daten in Frage und fordert die WADA auf sicherzustellen, dass diese Notwendigkeit gegeben ist. Sie empfiehlt in jedem Fall, dass bei der Verarbeitung der besagten Daten ein besonders hohes Datenschutzniveau eingehalten wird.

Artikel 6.4

Der Anwendungsbereich von Artikel 6.4 sollte erweitert werden, um den Rechtsvertretern der Teilnehmer die Möglichkeit zu geben, von den weiteren im Entwurf des Standards vorgesehenen Rechten Gebrauch zu machen, wie sie zum Beispiel unter Punkt 11 näher erläutert werden.

Punkt 7 – Die Weitergabe der erforderlichen Informationen an die Teilnehmer sicherstellen

Die Arbeitsgruppe verweist auf die Bestimmungen von Artikel 10 und Artikel 11 der Datenschutzrichtlinie, insbesondere auf die Regelung, dass neben der Identität des für die Datenverarbeitung Verantwortlichen auch die Identität seiner Vertreter mitzuteilen ist.

Artikel 7.2 sieht vor, dass die Teilnehmer „so bald wie möglich" unterrichtet werden, wenn an anderer Stelle als bei ihnen selbst personenbezogene Informationen über sie erhoben werden. Um die Anforderungen der Datenschutzrichtlinie (Artikel 11 Absatz 1) zu erfüllen, muss die betroffene Person diese Information bei Beginn der Speicherung der Daten bzw. im Fall einer beabsichtigten Weitergabe der Daten an Dritte spätestens bei der ersten Übermittlung erhalten. Unter bestimmten Voraussetzungen kann auf eine Übermittlung dieser Information verzichtet werden, *„wenn insbesondere bei Verarbeitungen für Zwecke der Statistik oder der historischen oder wissenschaftlichen Forschung die Information der betroffenen Person unmöglich ist, unverhältnismäßigen Aufwand erfordert oder die Speicherung oder Weitergabe durch Gesetz ausdrücklich vorgesehen ist"*. Diese Einschränkungen sind jedoch eng auszulegen.

Die Arbeitsgruppe macht ferner darauf aufmerksam, dass Formulierungen wie *„er/sie sollte (…) angemessenen Zugang zu Informationen erhalten …“* im Kommentar zu Artikel 7.2 das Informationsrecht der betroffenen Personen abschwächen. Sie weist darauf hin, dass das Recht der betroffenen Person auf Information unverzichtbar und Bestandteil der Anforderung ist, dass die Transparenz der Datenverarbeitung gewährleistet sein muss.

Punkt 8 – Offenlegung personenbezogener Informationen gegenüber anderen Anti-Doping-Organisationen und Dritten

Die Arbeitsgruppe hebt hervor, dass eine Weitergabe aus dem Europäischen Wirtschaftsraum an ein Drittland nur dann erfolgen kann, wenn das Drittland ein angemessenes Schutzniveau, wie in Artikel 25 Absatz 2 der Datenschutzrichtlinie beschrieben sicherstellt, oder wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre bietet, oder wenn die Übermittlung auf der Grundlage einer der Ausnahmeregelungen erfolgt, die in Artikel 26 Absatz 1 der Datenschutzrichtlinie vorgesehen sind.

Im vorliegenden Fall wird die Datenbank ADAMS in Kanada geführt. Im Sinne von Artikel 25 Absatz 2 der Datenschutzrichtlinie gilt Kanada als Land, das ein angemessenes Schutzniveau für personenbezogene Daten bietet, die von der Europäischen Union an Empfänger übermittelt werden, die dem kanadischen Personal Information Protection and Electronic Documents Act (PIPEDA)[3] unterliegen. Der Arbeitsgruppe ist allerdings nicht klar, ob die WADA oder eine nationale Anti-Doping-Behörde in Kanada als der für die Datenbank ADAMS Verantwortliche angesehen wird oder ob der für die Datenverarbeitung Verantwortliche den Bestimmungen des PIPEDA unterliegt. Die Arbeitsgruppe empfiehlt, dies klarzustellen und für den Fall, dass der Verantwortliche für die Datenbank ADAMS nicht dem PIPEDA unterliegt, weitere Schritte zu unternehmen, um sicherzustellen, dass ein angemessenes Schutzniveau für Daten gewährleistet ist, die von der Europäischen Union für die Datenbank ADAMS übermittelt werden.

Die Arbeitsgruppe betont, dass der „Grundsatz der Zweckbestimmung“ und die Anforderung der Vereinbarkeit der Verarbeitung von weitergegebenen Daten mit dem ursprünglichen Zweck, für die die Daten erhoben wurden, einzuhalten sind.

In Bezug auf Artikel 8.4 erinnert die Arbeitsgruppe an ihre Ausführungen zu Punkt 6 oben, die die Gültigkeit der Zustimmung betreffen. Die Arbeitsgruppe weist außerdem darauf hin, dass nach dieser Bestimmung eine Veröffentlichung von personenbezogenen Informationen über Athleten oder andere Personen im

[3] 2002/2/EG: Entscheidung der Kommission vom 20. Dezember 2001 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet (Bekannt gegeben unter Aktenzeichen K(2001) 4539).

Internet, wie sie Artikel 14.2.4 des Anti-Doping-Codes (siehe Punkt 2 oben – Bestimmungen des Codes) vorsieht, nicht zulässig ist.

Punkt 9 – Gewährleistung der Sicherheit von personenbezogenen Informationen

Was Punkt 9.1 anbelangt, sind die Kontaktdaten der von der Anti-Doping-Organisation eingesetzten Person unverzüglich an die Teilnehmer zu übermitteln (ebenso wie die unter Punkt 7.1 genannten Informationen), und zwar nicht nur, wenn sie diese Daten anfordern.

Zu den Auftragsverarbeitern, die von den Anti-Doping-Organisationen möglicherweise eingesetzt werden (Vertreter Dritter – Punkt 9.4), verweist die Arbeitsgruppe auf die Regeln, die in Artikel 16 und Artikel 17 der Datenschutzrichtlinie festgelegt sind, insbesondere auf die Verpflichtung des für die Datenverarbeitung Verantwortlichen, einen Auftragsverarbeiter auszuwählen, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet.

Punkt 10 – Personenbezogene Informationen nur soweit erforderlich speichern und die Vernichtung der Daten sicherstellen

Die Arbeitsgruppe begrüßt, dass in diese Fassung des Entwurfs eine Bestimmung aufgenommen wurde, die die Dauer der Speicherung von Daten und die Verpflichtung zur Löschung dieser Daten, wenn sie im Hinblick auf die Zwecke, für die sie verarbeitet wurden, nicht mehr benötigt werden regelt. Dennoch fordert sie die WADA auf, nach Möglichkeit und unter Berücksichtigung der auf diesem Gebiet bereits gesammelten Erfahrungen, einen angemessenen Zeitraum für die Speicherung dieser Daten – oder zumindest für bestimmte Datenkategorien – durch die Anti-Doping-Organisationen festzulegen. Punkt 2, der die Vorschriften für die Offenlegung in Artikel 14.2.4 des Anti-Doping-Codes betrifft, sollte hier nicht als Modell dienen. Diese Vorschriften erscheinen unverhältnismäßig, da sie vorsehen, dass die Veröffentlichung „zumindest" darin besteht, dass personenbezogene Informationen über Athleten oder andere Personen, die im Verdacht stehen, gegen Anti-Doping-Vorschriften verstoßen zu haben, „auf der Website der Anti-Doping-Organisation einzustellen und dort für mindestens ein Jahr zu belassen sind" (siehe oben, Teil I).

Die Arbeitsgruppe verweist zudem auf ihre Stellungnahme 4/2007 zum Begriff personenbezogene Daten[4], um besser zu verstehen, was mit *„Anonymisierung/ anonymen Daten"* im Sinne der Richtlinie gemeint ist.

4 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf

Punkt 11 – Rechte der Teilnehmer im Hinblick auf personenbezogene Informationen

Der Standard sieht für die Athleten und ihre Betreuer ein Auskunftsrecht vor. Gemäß Artikel 12 der Datenschutzrichtlinie hat jede betroffene Person insbesondere das Recht, vom für die Datenverarbeitung Verantwortlichen zumindest Informationen über die Zweckbestimmung der Verarbeitungen, die Kategorien der Daten, die Gegenstand der Verarbeitung sind, und die Empfänger oder Kategorien der Empfänger, an die Daten übermittelt werden, zu erhalten. Diese Elemente sind im Entwurf des Standards nicht enthalten.

Dem Entwurf zufolge sind die Anti-Doping-Organisationen in bestimmten Fällen nicht zur Beantwortung von Auskunftsersuchen verpflichtet. Die Arbeitsgruppe stellt in diesem Zusammenhang fest, dass die Ausnahmen in den Punkten 11.1 *(sofern dies in einem speziellen Fall die Fähigkeit der Anti-Doping-Organisation beeinträchtigen würde, ihren aus dem Code hervorgehenden Verpflichtungen nachzukommen)* und 11.2 *(Anträge, die eindeutig rechtsmissbräuchlich oder im Hinblick auf ihren Umfang oder ihre Häufigkeit überzogen sind oder, was die Kosten oder den Aufwand anbelangt, eine unverhältnismäßige Belastung darstellen)* sehr vage formuliert sind und bei oberflächlicher Betrachtung der Regelung nicht mit Artikel 12 und Artikel 15 der Richtlinie übereinstimmen. Beschränkungen des Auskunftsrechts sind grundsätzlich nur möglich, wenn sie im Einklang mit den Bestimmungen des Artikels 13 der Richtlinie stehen, der es den Mitgliedstaaten gestattet, Rechtsvorschriften zu erlassen, die diese Pflicht beschränken, sofern eine solche Beschränkung notwendig ist, um die in diesen Bestimmungen genannten Interessen zu schützen.

Die Arbeitsgruppe stellt mit Zufriedenheit fest, dass den Teilnehmer bei einer Verweigerung des Auskunftsrechts die Gründe für die Auskunftsverweigerung schriftlich mitgeteilt werden. Sie erinnert jedoch daran, dass eine solche Verweigerung nur unter den in Artikel 13 der Richtlinie genannten Bedingungen möglich ist, der eng auszulegen ist.

Zu Artikel 11.4 weist die Arbeitsgruppe darauf hin, dass gemäß Artikel 12 Buchstabe c) der Richtlinie der für die Datenverarbeitung Verantwortliche den Dritten, denen die Daten übermittelt wurden, jede Berichtigung, Löschung oder Sperrung von unvollständigen oder unrichtigen Daten mitteilen muss, sofern sich dies nicht als unmöglich erweist oder kein unverhältnismäßiger Aufwand damit verbunden ist. Um die Übereinstimmung mit der europäischen Datenschutzverordnung zu gewährleisten, sollte das Wort *„gegebenenfalls“* ausschließlich im Sinne dieser beiden Ausnahmen ausgelegt werden.

Zusätzliche Bestimmungen

Abschließend bedauert die Arbeitsgruppe, dass mehrere Grundsätze der europäischen Datenschutzvorschriften nicht in den Entwurf des Standards aufgenommen wurden. Sie bittet die WADA, die Aufnahme einer Reihe von zusätzlichen Bestimmungen zu prüfen, um Folgendes zu gewährleisten:

– das Verbot automatisierter Einzelentscheidungen (Artikel 15 der Richtlinie): Angesichts der Sanktionen, die die Datenverarbeitung zur Folge haben kann, erscheint dieses Verbot sehr wichtig.

– eine unabhängige Kontrolle, inwieweit die Mindestanforderungen des Standards durch die Anti-Doping-Organisationen umgesetzt werden. Nach Artikel 8.3 des Entwurfs des Standards können Anti-Doping-Organisationen die WADA unterrichten, wenn sie der Ansicht sind, dass andere Organisationen den Standard nicht einhalten. Die Arbeitsgruppe gibt zu bedenken, dass ein solcher Mechanismus für Informanten Zweifel daran weckt, ob die WADA ihre Zusage, für die wirksame Umsetzung und die Einhaltung der Bestimmungen des Standards zu sorgen, erfüllen wird. Sie stellt außerdem fest, dass bei Nichteinhaltung des Standards keinerlei Sanktionen gegen Anti-Doping-Organisationen vorgesehen sind. Abschließend stellt sich die Frage, wie wirksam dieser Standard sein wird.

– ein Widerspruchsrecht und ein Recht auf Entschädigung für Nachteile, die durch nicht dem Standard entsprechende Verarbeitungen entstanden sind.

– eine Regelung, die bewirkt, dass für nationale Anti-Doping-Organisationen die nationalen Rechtsvorschriften über die Verarbeitung personenbezogener Daten gelten.

***

Die Arbeitsgruppe unterstützt die Initiative der WADA, deren Ziel die Anwendung von Mindeststandards für den Schutz der Privatsphäre und den Schutz personenbezogener Daten von Athleten und anderen an der Dopingbekämpfung beteiligten Personen ist. Die Artikel-29-Arbeitsgruppe vertritt die Auffassung, dass dieser Standard angesichts seines geografischen Anwendungsbereichs eine wichtige Rolle bei der Verarbeitung von Daten spielen kann, die nicht den Rechtsvorschriften der EU oder einer von der EU als angemessen angesehenen Gesetzgebung unterliegt. Zudem wird dieser Standard in allen beteiligten Staaten – ob sie für die Datenverarbeitung einen angemessenen Schutz gewährleisten oder nicht – dazu beitragen, die Anti-Doping-Organisationen für dieses Thema zu sensibilisieren.

Die Arbeitsgruppe ist erfreut darüber, dass in der Präambel zu diesem Standard auf die Datenschutzrichtlinie verwiesen wird. Sie kann den Standard in der vorliegenden Form jedoch noch nicht uneingeschränkt unterstützen, da die darin festgelegten Mindestanforderungen allem Anschein nach nicht den in der europäischen Datenschutzverordnung verlangten Mindeststandards entsprechen. Allerdings ist eine solche Zustimmung denkbar, wenn die oben erläuterten Anmerkungen berücksichtigt und ausführlichere Angaben über die Datenbank ADAMS aufgenommen werden. Die Arbeitsgruppe fordert die WADA daher auf, diese Anmerkungen bei der Gestaltung des Entwurfs des Standards zu berücksichtigen. Sie bittet die WADA, ihr weitere Informationen zu übermitteln und ist zu einem Treffen mit der WADA bereit, falls dies zu diesem Zweck erforderlich sein sollte.

Dessen ungeachtet äußert die Arbeitsgruppe den Wunsch, weiterhin über die im Hinblick auf ihre Anmerkungen unternommenen Schritte und den allgemeinen Fortgang der Arbeit der WADA an diesem Entwurf für einen Standard informiert zu werden.

Brüssel, den 1. August 2008

Für die Arbeitsgruppe
Der Vorsitzende
Alex TÜRK

V. Internationale Konferenz der Datenschutzbeauftragten

Entschließungen der 30. Konferenz vom 15.–17. Oktober 2008

Entschließung über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen und die Erarbeitung einer gemeinsamen Entschließung zur Erstellung internationaler Normen zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten

Die Konferenz erinnert daran, dass:

– die auf ihrer 22. Konferenz in Venedig verabschiedete Erklärung;
– die auf ihrer 26. Konferenz in Breslau gefasste Entschließung;
– die auf ihrer 27. Konferenz in Montreux verabschiedete Erklärung;
– die auf ihrer 28. Konferenz vorgestellte Londoner Initiative;
– die auf ihrer 29. Konferenz gefasste Entschließung;

- den universellen Charakter des Rechts auf Datenschutz und auf den Schutz der Privatsphäre stärken wollen und zur Erstellung eines universellen Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten aufrufen.

- Insbesondere in der Erklärung von Montreux ruft die Konferenz die Organisation der Vereinten Nationen auf, ein zwingendes Rechtsinstrument auszuarbeiten, in dem das Recht auf Datenschutz und das Recht auf den Schutz der Privatsphäre als durchsetzbare Menschenrechte im Einzelnen festgeschrieben werden. Ferner ruft die Konferenz den Europarat auf, gemäß Artikel 23 des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten die Nichtmitgliedstaaten dieser Organisation, die eine entsprechende Datenschutzgesetzgebung besitzen, aufzufordern, dem Übereinkommen (STE Nr. 108) und seinem Zusatzprotokoll (STE Nr. 181) beizutreten.

- In der Entschließung der 29. Konferenz haben die Datenschutzbeauftragten die Notwendigkeit unterstrichen, die Erarbeitung effizienter, universell anerkannter internationaler Normen zum Schutz der Privatsphäre zu unterstützen, als Mechanismus, um den Parteien zu helfen, die Konformität mit den gesetzlichen Anforderungen im Bereich des Datenschutzes und des Schutzes der Privatsphäre herzustellen und nachzuweisen.

Die Konferenz stellt fest, dass inzwischen ermutigende Anstrengungen gemacht wurden, um diese Ziele zu erreichen und dass insbesondere:

- Die Frage eines universellen Übereinkommens auf dem Arbeitsprogramm der Kommission für internationales Recht der Vereinten Nationen steht;

- Der Europarat den Beitritt von Nichtmitgliedstaaten befürwortet, deren Datenschutzgesetzgebung den Anforderungen des Übereinkommens STE Nr. 108 entspricht, und beschlossen hat, sich für dieses Regelwerk weltweit einzusetzen; so hat er die potenziell universelle Gültigkeit des Übereinkommens STE Nr. 108 betont, insbesondere auf dem Weltgipfel zur Informationsgesellschaft in Tunis im November 2005 und bei den Foren zur Internet-Governance 2006 in Athen und 2007 in Rio;

- Die OECD am 12. Juni 2007 eine Empfehlung zur grenzübergreifenden Zusammenarbeit bei der Anwendung der Rechtsvorschriften zum Schutz der Privatsphäre angenommen hat, die insbesondere darauf abstellt, die nationalen Rahmen zur Anwendung der Gesetze über den Schutz der Privatsphäre zu verbessern, um eine bessere Zusammenarbeit der nationalen Behörden mit den ausländischen Behörden zu ermöglichen, und wirksame internationale Mechanismen zu erarbeiten, um die grenzübergreifende Zusammenarbeit zur Anwendung der Gesetze zum Schutz der Privatsphäre zu erleichtern;

- Die Regionalkonferenzen der Unesco 2005 (Asien-Pazifik) und 2007 (Europa) den prioritären Charakter des Datenschutzes unterstreichen;

- Die Artikel 29-Gruppe der Europäischen Union Initiativen ergriffen hat, um das Verabschiedungsverfahren für zwingende Vorschriften für Unternehmen (BCR) und die Entwicklung vertraglicher Lösungen für den grenzübergreifenden Datenaustausch zu erleichtern.

- Die Staats- und Regierungschefs der „Frankophonie“ sich zum Abschluss ihres 11. Gipfels im September 2006 in Budapest verpflichtet haben, auf nationaler Ebene die Arbeit an den erforderlichen gesetzlichen und verordnungsrechtlichen Regelungen zur Festschreibung des Rechtes der Menschen auf Datenschutz zu intensivieren und sich weltweit für die Ausarbeitung eines internationalen Übereinkommen einzusetzen, das die Effektivität des Rechts auf Datenschutz gewährleistet;

- Die APEC im November 2004 Leitprinzipien zum Schutz der Privatsphäre verabschiedet hat, um den Schutz der Privatsphäre zu verstärken und den Informationsfluss aufrechtzuerhalten. Im September 2007 hat die APEC eine Initiative „Privatsphäre“ zur Entwicklung des Umsetzungsrahmens gestartet, um zertifizierte internationale Datenflüsse sicherzustellen, die den Bedürfnissen

des Geschäftsverkehrs entsprechen, die Konformitätskosten senken, den Verbrauchern ein wirksames Instrument an die Hand geben, den Regulatoren effizientes Handeln ermöglichen und die Vorschriftenlast verringern;

- Die in Montreal am Rande der 29. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre gegründete Frankophone Vereinigung der Datenschutzbehörden (AFAPDP) in ihren Zielsetzungen die Ausarbeitung eines universellen Übereinkommens und die Bemühungen mit Blick auf den Beitritt von Nichtmitgliedstaaten des Europarats zum Übereinkommen STE Nr. 108 unterstützt;

- Das Iberoamerikanische Datenschutz-Netzwerk (RIPD) zum Abschluss seiner 6. Tagung im Mai 2008 in Kolumbien eine Erklärung angenommen hat, in der die internationalen Konferenzen für den Datenschutz und für die Privatsphäre aufgerufen werden, unabhängig von ihrer geografischen Zugehörigkeit ihre Bemühungen mit dem Ziel der Verabschiedung eines gemeinsamen Rechtsinstruments fortzusetzen;

- Die mittel- und osteuropäischen Datenschutzbehörden (APDCO) auf ihrer jüngsten Tagung im Juni 2008 in Polen ihren Willen bekundet haben, ihre Aktivitäten im Rahmen von APDCO fortzusetzen und zu verstärken und insbesondere gemeinsame Lösungen zu erarbeiten und die neuen Mitglieder bei der Implementierung ihrer Datenschutzgesetzgebung zu unterstützen.

Die Konferenz ist der Ansicht, dass:

- das Recht auf Datenschutz und den Schutz der Privatsphäre ein Grundrecht der Menschen ist, unabhängig von ihrer Staatsangehörigkeit und ihrem Wohnsitz;

- in der sich ausbreitenden Informationsgesellschaft das Recht auf Datenschutz und auf den Schutz der Privatsphäre in einer demokratischen Gesellschaft eine unerlässliche Voraussetzung ist, um die Achtung der Rechte der Personen, den freien Fluss von Informationen und eine offene Marktwirtschaft zu gewährleisten;

- die Globalisierung des Austauschs und der Verarbeitung personenbezogener Daten, die Komplexität der Systeme, die Schäden, die durch eine unangemessene Nutzung immer leistungsfähigerer Technologien entstehen können und der Anstieg der Sicherheitsmaßnahmen eine rasche und angemessene Antwort erfordern, um die Achtung der Grundrechte und -freiheiten, insbesondere des Rechts auf Schutz der Privatsphäre, zu gewährleisten;

- die anhaltenden Disparitäten im Bereich des Datenschutzes und der Achtung der Privatsphäre weltweit, insbesondere wegen des Fehlens von Garantien in mehreren Staaten, dem Austausch personenbezogener Daten und der Schaffung eines effizienten, globalen Datenschutzes schaden;

- die Entwicklung internationaler Regeln, die die Achtung des Datenschutzes und des Schutzes der Privatsphäre einheitlich gewährleisten, eine Priorität darstellt;

- die Anerkennung dieser Rechte die Verabschiedung eines universellen, zwingenden Rechtsinstruments erfordert, das die in den verschiedenen bestehenden Instrumenten festgeschriebenen gemeinsamen Prinzipien des Datenschutzes und der Achtung der Privatsphäre bestätigt, auflistet und ergänzt und die internationale Zusammenarbeit zwischen Datenschutzbehörden verstärkt;

- die Umsetzung der von Organisationen wie der APEC oder der OECD entwickelten Leitlinien, insbesondere derjenigen, die die Annahme eines internationalen Rahmens zur Verbesserung der Achtung des Rechts auf Datenschutz und auf den Schutz der Privatsphäre bei grenzüberschreitenden Datenflüssen betreffen, eine positive Etappe zur Erreichung dieses Ziels darstellt;

- der Beitritt zu zwingenden Instrumenten mit universeller Gültigkeit, wie das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (STE Nr. 108) und sein Zusatzprotokoll über die Kontrollbehörden und den grenzüberschreitenden Datenfluss (STE Nr. 181), die Grundprinzipien des Datenschutzes enthalten, den Austausch von Daten zwischen Parteien erleichtern kann; diese Instrumente sehen in der Tat Mechanismen und eine Plattform für die Zusammenarbeit zwischen den Datenschutzbehörden vor, tragen Sorge dafür, dass diese Behörden bei der Erfüllung ihrer Aufgaben völlig unabhängig sind und fördern die Einrichtung eines angemessenen Datenschutzniveaus;

- die 30. Internationale Datenschutzkonferenz eine geeignete Instanz für die Verabschiedung einer Strategie ist, die speziell auf die Verwirklichung dieser Ziele ausgerichtet ist.

Daher erneuert die Konferenz **ihren Appell**, ein zwingendes, universelles Rechtsinstrument zum Datenschutz und zum Schutz der Privatsphäre auszuarbeiten und **fasst dazu folgende Entschließungen**:

1. Die Konferenz unterstützt die Bemühungen des Europarats, das Grundrecht auf Datenschutz und auf den Schutz der Privatsphäre zu fördern. Die Konferenz fordert daher die Mitgliedstaaten dieser Organisation, die dies noch

nicht getan haben, auf, die Ratifizierung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und ihres Zusatzprotokolls zu prüfen. Die Konferenz fordert die Nichtmitgliedstaaten, die in der Lage sind, es zu tun, auf, zu erwägen, der Einladung des Europarats, dem Übereinkommen STE Nr. 108 und seinem Zusatzprotokoll beizutreten, Folge zu leisten. Mit Blick auf ihre Entschließung über die Errichtung einer Lenkungsgruppe zur Vertretung bei Tagungen internationaler Organisationen hat die Konferenz den Wunsch, auch einen Beitrag zu den Arbeiten des beratenden Ausschusses des Übereinkommens STE Nr. 108 zu leisten.

2. Die Konferenz unterstützt die Initiativen der APEC, der OECD und anderer regionaler Organisationen und internationaler Foren für die Entwicklung wirksamer Mittel zur Förderung besserer internationaler Standards für den Datenschutz und den Schutz der Privatsphäre.

3. **Die Konferenz beauftragt** eine Arbeitsgruppe, die von der den 31. Internationalen Konferenz ausrichtenden Behörde koordiniert wird und sich aus den interessierten nationalen Datenschutzbehörden zusammensetzt, einen **gemeinsamen Vorschlag zur Erstellung internationaler Normen zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten** abzufassen und ihr auf ihrer nichtöffentlichen Sitzung vorzulegen, wobei folgender Kriterien vorgegeben werden:

   - Vornahme einer Bestandsaufnahme der Grundsätze und Rechte im Bereich des Schutzes personenbezogener Daten in den verschiedenen geografischen Gebieten der Welt, wobei besonders auf Gesetzestexte oder andere Texte abzustellen ist, die in den regionalen und internationalen Foren auf weitgehenden Konsens gestoßen sind;

   - Erarbeitung einer Zusammenstellung von Prinzipien und Rechten, die die bestehenden Texte widerspiegelt und ergänzt und dadurch die Erreichung eines Höchstmaßes an internationaler Akzeptanz zur Sicherung eines hohen Schutzniveaus ermöglicht;

   - Beurteilung der Sektoren, in denen diese Rechte und Prinzipien Anwendung finden, einschließlich der Varianten, die den Akzent auf die Harmonisierung ihrer Anwendungsbereiche legen;

   - Bestimmung der grundlegenden Kriterien, die ihre tatsächliche Anwendung gewährleisten, unter Berücksichtigung der Verschiedenheit der Rechtssysteme;

   - Prüfung der Rolle, die die Selbstregulierung spielen muss;

- Formulierung wesentlicher Garantien für bessere und flexiblere internationale Datentransfers.

Bei dem Verfahren, das zur Abfassung dieses gemeinsamen Vorschlags führt, sollen die öffentlichen und privaten Organisationen und Instanzen zu einer breiten Beteiligung an den Arbeitsgruppen und an Foren und Anhörungen ermutigt werden, um zu einem möglichst umfassenden institutionellen und gesellschaftlichen Konsens zu gelangen. Besondere Aufmerksamkeit sollte den laufenden Arbeiten der Internationalen Organisation für Normung (ISO) und der Kommission für internationales Recht gewidmet werden.

Entschließung zum Schutz der Privatsphäre von Kindern im Internet

Überall in der Welt gehen die Jugendlichen von zu Hause und von der Schule aus sowie über ihre kabellosen Geräte ins Internet. Sie nutzen das Internet zur sozialen Interaktion – sie tauschen Geschichten, Ideen, Fotos und Videos aus, sie bleiben den Tag über durch SMS-Mitteilungen in Kontakt mit ihren Freunden und sie beteiligen sich an Online-Spielen gemeinsam mit anderen Personen am anderen Ende der Welt.

Dabei werden die Jugendlichen auch mit den Schwierigkeiten und Herausforderungen bezüglich des Schutzes ihrer persönlichen Daten im Internet konfrontiert. Das Fehlen einer Regelung bei zahlreichen Internetdiensten macht die Sache schwierig. Viele der bei Jugendlichen beliebtesten Websites sammeln große Mengen personenbezogener Daten für Verkaufs- und Marketingzwecke.

Mit steigender Anzahl der im Internet angebotenen Anwendungen und Technologien wird die Menge der gesammelten und aufbewahrten personenbezogenen Daten immer größer. Heute sind sich die Jugendlichen oft nicht darüber bewusst, dass ihre Auskünfte, ihre Gewohnheiten und ihre Verhaltensweisen im Internet überwacht werden.

Untersuchungen zeigen, dass die Jugendlichen (wie auch zahlreiche Erwachsene) nur selten die Geheimhaltungserklärungen der von ihnen besuchten Websites lesen, was nicht überrascht, denn die Vertraulichkeitserklärungen zahlreicher Websites sind in einer technischen oder juristischen Fachsprache abgefasst, die für die meisten Leser schwer verständlich ist.

Wenn auch manche Jugendliche die mit ihren Online-Aktivitäten verbundenen Gefahren erkennen, so verfügen sie doch nicht über die Erfahrung, die technischen Kenntnisse oder die nötigen Instrumente, um diese Gefahren zu mindern. Oft kennen sie ihre gesetzlichen Rechte nicht.

Vor fast 20 Jahren hat die Generalversammlung der Vereinten Nationen 1989 ein Übereinkommen über die Rechte des Kindes verabschiedet. In diesem heißt es, dass die Staaten die Rechte des Kindes achten und schützen müssen, einschließlich ihres Rechtes auf den Schutz ihrer Privatsphäre.

Seit dieser Zeit bereiteten den Datenschutzbeauftragten die Verletzungen der Privatsphäre von Kindern im Internet immer mehr Sorgen. In der am 20. Februar 2008 vom Ministerrat des Europarats angenommenen Erklärung zum Schutz der Würde, Sicherheit und der Privatsphäre von Kindern im Internet zeigt sich dieser von der Notwendigkeit überzeugt, Kinder über die lange Speicherdauer und über die Risiken der von ihnen ins Internet eingestellten Inhalte aufzuklären. Er erklärte darüber hinaus, dass, anders als bei der Strafverfolgung, keine fortbestehenden oder dauerhaft zugänglichen Aufzeichnungen über die von Kindern ins Internet eingestellten Inhalte existieren sollten, die deren Würde, Sicherheit und Privatsphäre angreifen oder ihnen auf andere Art und Weise jetzt oder zu einem späteren Zeitpunkt ihres Lebens schaden können.

Die Datenschutzbeauftragten haben zugleich erkannt, dass ein auf Erziehung ausgerichteter Ansatz, verbunden mit einer Regelung des Datenschutzes, eine der wirksamsten Methoden zur Bewältigung dieses Problems darstellt. So haben mehrere Länder innovative, auf Erziehung angelegte Konzepte umgesetzt, um der Herausforderung zu begegnen, die der Schutz der Privatsphäre von Kindern im Internet darstellt.

Kinder und Jugendliche haben ein Recht darauf, sich online sicher bewegen und positive Erfahrungen machen zu können, bei denen sie die Absichten der Personen, mit denen sie interagieren, kennen und verstehen.

Die auf der 30. internationalen Konferenz versammelten Beauftragten für den Datenschutz und für die Privatsphäre haben beschlossen:

– die Erarbeitung von Ansätzen zu fördern, die auf Erziehung angelegt sind, um die Lage in Bezug auf den Schutz der Privatsphäre im Internet auf nationaler wie auf internationaler Ebene zu verbessern;

– bemüht zu sein, dafür zu sorgen, dass Kinder und Jugendliche in der ganzen Welt Zugang zu einem sicheren Online-Umfeld haben, das ihre Privatsphäre respektiert;

– mit Partnern und Akteuren im eigenen Land und im Ausland zusammenzuarbeiten, in der Erkenntnis, dass die Zusammenarbeit mit den Fachleuten, die das tägliche Leben der Kinder beeinflussen, von entscheidender Bedeutung ist;

– miteinander zu arbeiten, um beispielhafte Praktiken auszutauschen und Aktivitäten zur Erziehung der Öffentlichkeit durchzuführen, um Kinder und Jugendliche stärker zu sensibilisieren hinsichtlich der Gefahren in Bezug auf den Schutz ihrer Privatsphäre, die mit ihren Online-Aktivitäten verbunden sind, und bezüglich der sich ihnen bietenden Möglichkeiten einer aufgeklärten Wahl, um ihre persönlichen Informationen zu kontrollieren;

– bei Erziehenden die Einsicht zu fördern, dass die Sensibilisierung für den Schutz der Privatsphäre einen wesentlichen Aspekt der Kindererziehung darstellt und in ihr Unterrichtsprogramm aufgenommen werden muss;

– zu fordern, dass die Behörden Gesetze erlassen, die die Sammlung, Verwendung und Mitteilung personenbezogener Daten von Kindern einschränken, einschließlich geeigneter Bestimmungen für den Fall von Verstößen;

– bei Online-Werbung für Kinder oder verhaltensbezogener Werbung geeignete Einschränkungen bei der Sammlung, Verwendung und Mitteilung personenbezogener Daten von Kindern zu fordern;

– die Betreiber von Websites für Kinder anzuhalten, ihr soziales Bewusstsein unter Beweis zu stellen, indem sie Vertraulichkeitserklärungen und Nutzungsvereinbarungen einführen, die klar, einfach und verständlich sind und indem sie die Nutzer über die Gefahren für den Schutz der Privatsphäre und die Sicherheit sowie über die ihnen auf der Website gebotenen Wahlmöglichkeiten aufklären.

Entschließung zum Datenschutz in Sozialen Netzwerkdiensten

Soziale Netzwerkdienste[1] haben in den letzten Jahre große Beliebtheit erworben. Diese Dienste bieten ihren Teilnehmern Interaktionsmöglichkeiten auf der Basis von selbst generierten persönlichen Profilen, die in einem noch nie da gewesenen Ausmaß die Veröffentlichung persönlicher Informationen zu den betreffenden Personen (und auch anderen Personen) mit sich bringen. Die sozialen Netzwerkdienste bieten zwar ein neues Spektrum von Möglichkeiten für Kommunikation und den Echtzeit-Austausch von Informationen jeder Art, die Nutzung dieser Dienste kann jedoch auch eine Gefährdung der Privatsphäre ihrer Nutzer – und Anderer – mit sich bringen, denn personenbezogene Daten einzelner Personen werden in bisher unbekannter Weise und Menge öffentlich (und global) zugänglich, einschließlich großer Mengen digitaler Fotos und Videos.

[1] „Ein sozialer Netzwerkdienst stellt ab auf den Aufbau […] sozialer Online-Netzwerke für Gruppen von Menschen, die gemeinsame Interessen und Aktivitäten teilen oder daran interessiert sind, die Interessen und Aktivitäten Anderer zu erkunden […]. Die meisten Dienste sind hauptsächlich webbasiert und bieten Nutzern eine Reihe verschiedener Interaktionsmöglichkeiten […]". Zitat aus Wikipedia: http://en.wikipedia.org/wiki/Social_network_service.

Der Einzelne läuft Gefahr, die Kontrolle über die Nutzung der Daten durch Andere zu verlieren, wenn sie erst einmal im Netzwerk publiziert sind: Während der Community-Bezug sozialer Netzwerke die Vorstellung erweckt, die Veröffentlichung der eigenen persönlichen Daten laufe in etwa auf das Gleiche hinaus, wie früher das Mitteilen von Information unter Freunden von Angesicht zu Angesicht, können Profildaten tatsächlich für alle Teilnehmer einer Community (deren Zahl in die Millionen gehen kann) verfügbar sein.

Derzeit gibt es wenig Schutz dagegen, dass personenbezogene Daten jeder Art aus Profilen kopiert werden – durch andere Mitglieder des Netzwerks oder durch unbefugte netzwerkfremde Dritte – und zum Aufbau von Persönlichkeitsprofilen verwendet werden oder dass die Daten anderweitig wieder veröffentlicht werden. Es kann sehr schwierig – und manchmal unmöglich – sein zu erreichen, dass Daten, wenn sie einmal publiziert sind, wieder vollständig aus dem Internet entfernt werden. Selbst nach ihrer Löschung auf der ursprünglichen Website (z. B. dem sozialen Netzwerk) können Kopien bei Dritten oder bei den Anbietern der sozialen Netzwerkdienste verbleiben. Personenbezogene Daten aus Nutzerprofilen können auch außerhalb des Netzwerks bekannt werden, wenn sie von Suchmaschinen indexiert werden. Hinzu kommt, dass manche Anbieter sozialer Netzwerkdienste über Applikationsprogrammierschnittstellen Drittanbietern Nutzerdaten zur Verfügung stellen, die dann unter der Kontrolle dieser Dritten stehen.

Ein Beispiel von Wiederverwendungen, das großes öffentliches Aufsehen erregt hat, ist die Praxis von Personalverantwortlichen, Nutzerprofile von Stellenbewerbern oder Angestellten zu durchsuchen. Presseberichten zufolge gibt bereits heute ein Drittel der Personalverantwortlichen an, bei ihrer Arbeit Daten aus sozialen Netzwerkdiensten zu nutzen, z. B. um die einzelnen Angaben von Bewerbern zu überprüfen und/oder zu ergänzen.

Profilinformationen und Verkehrsdaten werden von Anbietern sozialer Netzwerkdienste auch zur Weiterleitung zielgerichteter Werbung an ihre Nutzer verwendet.

Sehr wahrscheinlich werden in Zukunft noch weitere unerwartete Verwendungen von Informationen in Nutzerprofilen auftreten.

Zu weiteren, bereits jetzt identifizierten spezifischen Risiken für Datenschutz und Datensicherheit zählen erhöhte Risiken durch Identitätsbetrug, der durch die umfangreiche Verfügbarkeit personenbezogener Daten in Nutzerprofilen begünstigt wird, und durch eine mögliche Übernahme von Profilen durch unbefugte Dritte. Die 30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre erinnert daran, dass diese Risiken bereits in dem Dokument “Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten”

("Rom-Memorandum")[2] der 43. Tagung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommuniktion (3. - 4. März 2008) und in dem ENISA Positionspapier Nr. 1 „Security Issues and Recommendations for Online Social Networks"[3] (Oktober 2007) analysiert wurden.

Die in der Internationalen Konferenz versammelten Datenschutzbeauftragten sind von der Notwendigkeit überzeugt, dass als Erstes eine intensive Informationskampagne unter Beteiligung aller öffentlichen und privaten Interessengruppen – von Regierungsstellen bis zu Bildungseinrichtungen wie Schulen, von Anbietern sozialer Netzwerkdienste bis zu Verbraucher- und Nutzerverbänden, einschließlich der Datenschutzbeauftragten selbst – durchgeführt werden muss, um den vielfältigen mit der Nutzung sozialer Netzwerkdienste verbundenen Gefahren vorzubeugen.

Empfehlungen

In Anbetracht der besonderen Natur der Dienste und der kurz- und langfristigen Gefahren für die Privatsphäre des Einzelnen richtet die Konferenz folgende Empfehlungen an Nutzer und Anbieter sozialer Netzwerkdienste:

Nutzer sozialer Netzwerkdienste

Organisationen, denen am Wohl der Nutzer sozialer Netzwerke gelegen ist – einschließlich Diensteanbieter, Regierungen und Datenschutzbehörden – sollten mithelfen, die Nutzer über den Schutz ihrer personenbezogenen Daten aufzuklären und die folgende Botschaften zu vermitteln.

1. Veröffentlichung von Daten

Nutzer sozialer Netzwerkdienste sollten sich sorgfältig überlegen, welche persönlichen Daten sie – wenn überhaupt – in einem sozialen Netzwerkprofil publizieren. Sie sollten bedenken, dass sie zu einem späteren Zeitpunkt mit einer Information oder mit Bildern konfrontiert werden könnten, z. B. wenn sie sich um eine Arbeitsstelle bewerben. Insbesondere sollten Minderjährige vermeiden, ihre Privatanschrift oder ihre Telefonnummer mitzuteilen.

Privatpersonen sollten sich überlegen, ob es nicht ratsam wäre, in einem Profil anstelle ihres wirklichen Namens ein Pseudonym zu verwenden. Dabei sollten sie

2 http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491

3 http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

jedoch nicht vergessen, dass auch die Benutzung von Pseudonymen nur einen begrenzten Schutz gewährt, da Dritte in der Lage sein können, ein solches Pseudonym aufzudecken.

2. Die Privatsphäre Anderer

Nutzer sollten auch die Privatsphäre Anderer achten. Sie sollten besonders vorsichtig sein bei der Veröffentlichung personenbezogener Daten Anderer (einschließlich Bildern, oder sogar mit Zusatzinformationen versehenen Bildern) ohne die Einwilligung der betreffenden Personen.

Anbieter sozialer Netzwerkdienste

Anbieter sozialer Netzwerkdienste tragen eine besondere Verantwortung dafür, die Belange von Personen, die soziale Netzwerke nutzen, zu beachten und zu wahren. Sie sollten nicht nur die Regelungen des Datenschutzrechts einhalten, sondern auch die folgenden Empfehlungen umsetzen.

1. Datenschutzvorschriften und -standards

Anbieter, die in verschiedenen Ländern oder sogar weltweit tätig sind, sollten die Datenschutzstandards der Länder einhalten, in denen sie ihre Dienste betreiben. Zu diesem Zweck sollten die Anbieter Datenschutzbehörden konsultieren, wenn und soweit dies notwendig ist.

2. Aufklärung der Nutzer

Anbieter sozialer Netzwerkdienste sollten ihre Nutzer über die Verarbeitung ihrer personenbezogenen Daten transparent und offen informieren. Es sollte auch aufrichtig und verständlich über mögliche Folgen einer Veröffentlichung persönlicher Daten in einem Profil und über verbleibende Sicherheitsrisiken sowie über gesetzliche Zugriffsrechte Dritter (einschließlich z. B. von Strafverfolgungsbehörden) aufgeklärt werden. Eine solche Aufklärung sollte auch Hinweise dazu enthalten, wie Nutzer mit personenbezogenen Daten von Dritten umgehen sollten, die in ihren Profilen enthalten sind.

3. Nutzerkontrolle

Anbieter sollten die Kontrolle der Nutzer über die Verwendung ihrer Profildaten durch andere Community-Mitglieder weiter verbessern. Sie sollten die Einschränkung der Sichtbarkeit ganzer Profile sowie von in Profilen enthaltenen Daten, und in Community-Suchfunktionen ermöglichen.

Die Anbieter sollten auch eine Kontrolle der Nutzer über die Nutzung von Profil- und Verkehrsdaten, z. B. für zielgerichtete Werbung, ermöglichen. Als ein Minimum sollten eine Opt-out-Möglichkeit für allgemeine Profildaten und eine Opt-in-Möglichkeit für sensible Profildaten (z. B. politische Überzeugungen, sexuelle Orientierung) und Verkehrsdaten geboten werden.

4. Datenschutzfreundliche Standardeinstellungen

Darüber hinaus sollten Anbieter datenschutzfreundliche Standardeinstellungen für Nutzerprofilinformationen anbieten. Standardeinstellungen spielen eine Schlüsselrolle beim Schutz des Privatsphäre der Nutzer: Es ist bekannt, dass lediglich eine Minderheit von Nutzern, die sich bei einem Dienst anmelden, irgendwelche Änderungen daran vornimmt. Diese Einstellungen müssen bei einem sozialen Netzwerkdienst, der sich an Minderjährige wendet, besonders restriktiv sein.

5. Sicherheit

Anbieter sollten die Sicherheit ihrer Informationssysteme weiter verbessern und aufrechterhalten und die Nutzer gegen betrügerische Zugriffe auf ihre Profile schützen, indem sie für die Konzeption, die Entwicklung und den Betrieb ihrer Anwendungen anerkannte Methoden einschließlich unabhängigem Auditing und unabhängiger Zertifizierung verwenden.

6. Auskunftsrechte

Anbieter sollten Personen (gleichgültig ob Mitglieder des sozialen Netzwerkdienstes oder nicht) ein Recht auf Auskunft zu ihren personenbezogenen Daten gewähren und erforderlichenfalls diese Daten berichtigen.

7. Löschung von Nutzerprofilen

Anbieter sollten den Nutzern die Möglichkeit geben, ihre Mitgliedschaft auf einfache Weise zu beenden und ihre Profile sowie alle Inhalte oder Informationen, die sie in dem sozialen Netzwerk publiziert haben, zu löschen.

8. Pseudonyme Nutzung des Dienstes

Anbieter sollten als Option die Möglichkeit der Einrichtung und Verwendung pseudonymer Profile anbieten und zur Nutzung dieser Option ermutigen.

9. Zugriff durch Drittpersonen

Anbieter sollten wirksame Maßnahmen ergreifen, um das Durchsuchen und/oder massenweise Herunterladen (oder „bulk harvesting“) von Profildaten durch Dritte zu verhindern.

10. Indexierbarkeit der Nutzerprofile

Die Anbieter sollten sicherstellten, dass Nutzerdaten von externen Suchmaschinen nur durchsucht werden können, wenn der Nutzer dazu seine ausdrückliche, vorherige und informierte Einwilligung erteilt hat. Die Nichtindexierbarkeit von Profilen durch Suchmaschinen sollte als Standard eingestellt sein.

VI. Arbeitspapiere der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation

43. Sitzung am 3./4. März 2008 in Rom

Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten – *„Rom Memorandum“* –

– Übersetzung –

Bericht

Hintergrund

„Das Hauptaugenmerk eines sozialen Netzwerkdienstes ist auf die Bildung und Bestätigung von sozialen Beziehungen im Online-Bereich von Menschen gerichtet, die Interessen und Aktivitäten teilen, oder die an der Erkundung von Interessen und Aktivitäten anderer interessiert sind, und die Nutzung von Software voraussetzt. Die meisten Dienste sind im Wesentlichen webbasiert und bestehen in einer Ansammlung unterschiedlicher Möglichkeiten für Nutzer, zu interagieren […][1]. Insbesondere ermöglichen viele populäre Websites eine Interaktion mit anderen Nutzern (auf der Basis von selbstgenerierten persönlichen Profilen[2].

Das Aufkommen und die ständig wachsende Popularität sozialer Netzwerkdienste kündigt eine grundlegende Veränderung in Bezug auf die Art und Weise an, wie personenbezogene Daten großer Bevölkerungsgruppen in aller Welt mehr oder weniger öffentlich verfügbar werden. Diese Dienste sind in den letzten Jahren unglaublich populär geworden, insbesondere bei jungen Leuten. Sie werden aber auch zunehmend zum Beispiel im beruflichen Kontext oder für Senioren angeboten.

Die Herausforderungen, die soziale Netzwerkdienste stellen, sind auf der einen Seite nur eine weitere Variation der fundamentalen Veränderung, die die Entwicklungen des Internet in den 90er Jahren des letzten Jahrhunderts mit sich gebracht haben, in dem – unter anderem – Zeit und Raum bei der Veröffentlichung von Informationen und bei Echtzeitkommunikation aufgehoben wurden, und durch die Verwischung der Trennlinie zwischen Diensteanbietern (Autoren) einerseits und Nutzern/Konsumenten (Lesern) auf der anderen Seite.

1 zitiert aus Wikipedia; http://en.wikipedia.org/wiki/Social_network_service [abgerufen am 5. Februar 2008]

2 Dieser Bericht beschäftigt sich nicht mit Chat, Blogging und Bewertungsplattformen

Gleichzeitig scheinen soziale Netzwerkdienste die Grenzen dessen zu verändern, was gesellschaftlich als die Privatsphäre von Personen gesehen wird: Personenbezogene Daten über Einzelne werden öffentlich (und global) in einer nie vorher da gewesenen Weise und Menge[3] verfügbar, insbesondere riesige Mengen digitaler Bilder und Videos. Im Hinblick auf den Schutz der Privatsphäre könnte eine der grundlegendsten Herausforderungen in der Tatsache gesehen werden, dass die meisten der personenbezogenen Informationen, die in sozialen Netzwerkdiensten publiziert werden, auf Initiative der Nutzer selbst und mit ihrer Einwilligung veröffentlicht werden. Während die „traditionelle" Datenschutzgesetzgebung sich mit der Definition von Regeln zum Schutz der Bürger gegen unfaire oder unverhältnismäßige Verarbeitung personenbezogener Daten durch die öffentliche Verwaltung (einschließlich Strafverfolgungsbehörden und Geheimdienste), und von Unternehmen beschäftigt, gibt es nur sehr wenige Regelungen zur Veröffentlichung personenbezogener Daten auf Initiative der Betroffenen selbst, weil dies vor der Entwicklung sozialer Netzwerkdienste weder in der „Offline-Welt" noch im Internet ein großes Problem darstellte. Außerdem ist die Verarbeitung personenbezogener Daten aus öffentlichen Quellen traditionell in der Datenschutzgesetzgebung privilegiert.

Gleichzeitig ist eine neue Generation von Nutzern entstanden: Die erste Generation, die aufgewachsen ist, während das Internet bereits existierte. Diese „digitalen Eingeborenen"[4] haben ihre eigene Art der Nutzung von Internet-Diensten entwickelt, und eigene Ansichten darüber, was sie als der privat- bzw. der öffentlichen Sphäre zugehörig empfinden. Darüber hinaus könnten sie – da die meisten von ihnen im Teenager-Alter sind – eher bereit seien, Datenschutzrisiken einzugehen, als die älteren „digitalen Einwanderer". Generell scheint es, als seien jüngere Leute eher zur Veröffentlichung (manchmal intimer) Einzelheiten über ihr Leben im Internet bereit.

Gesetzgeber, Datenschutzbehörden wie auch Anbieter sozialer Netzwerkdienste sind mit einer Situation konfrontiert, die kein sichtbares Beispiel in der Vergangenheit hat. Während soziale Netzwerkdienste eine neue Bandbreite von Möglichkeiten für die Kommunikation und den Austausch von allen Arten von Informationen in Echtzeit bieten, kann die Nutzung solcher Dienste auch zu Gefährdungen der Privatsphäre der Nutzer (und anderer Bürger, die nicht einmal Teilnehmer an sozialen Netzwerkdiensten sind) führen.

---

[3] Ein deutscher Wissenschaftler hat kürzlich in einer Auswahl populärer sozialer Netzwerkdienste ungefähr 120 einzelne persönliche Attribute identifiziert, die in Nutzerprofilen sozialer Netzwerkdienste enthalten sind, wie z. B. Name, Privatadresse, Lieblingsfilme, -bücher und -musik usw., wie auch politische Ansichten und sogar sexuelle Vorlieben. Vgl. „Berliner Morgenpost" vom 23. Januar 2008, S. 9: „Mehr Informationen als die Stasi"; http://www.morgenpost.de/content/2008/01/23/wissenschaft/942868.html.

[4] Dieser Begriff wird Marc Prensky zugeschrieben, einem amerikanischen Redner, Autor, Berater und Spieledesigner im Bereich Ausbildung und Bildung. Vgl. z. B. http://www.ascd.org/authors/ed_lead/el200512_prensky.html [abgerufen am 5. Februar 2008]

Datenschutz- und Datensicherheitsrisiken

Die Ausbreitung sozialer Netzwerkdienste hat gerade erst begonnen. Während es bereits jetzt möglich ist, einige Risiken zu identifizieren, die mit dem Angebot und der Nutzung solcher Dienste verbunden sind, ist es sehr wahrscheinlich, dass wir gegenwärtig nur die Spitze des Eisbergs sehen, und dass sich in der Zukunft neue Nutzungen – und damit auch neue Risiken – entwickeln. Insbesondere werden neue Nutzungsformen für die in Nutzerprofilen enthaltenen personenbezogenen Daten durch die öffentliche Verwaltung (einschließlich Strafverfolgungsbehörden und Geheimdiensten[5]), wie auch durch den privaten Sektor, entwickelt werden.

Die folgende Liste von Risiken stellt nur eine Momentaufnahme dar, die möglicherweise mit der Weiterentwicklung sozialer Netzwerkdienste überarbeitet und aktualisiert werden muss.

Risiken in Verbindung mit der Nutzung sozialer Netzwerke, die bisher identifiziert worden sind, schließen die Folgenden ein:

1. *Im Internet gibt es kein Vergessen:* Die Idee des Vergessens ist im Internet nicht existent. Wenn Daten einmal publiziert sind, können sie dort sozusagen „bis in alle Ewigkeit" gespeichert bleiben – sogar dann, wenn der Betroffene sie von der ursprünglichen Website gelöscht hat, könnten Kopien bei Dritten existieren (einschließlich Archivdienste und die „Cache-Funktion", die von einem bekannten Suchmaschinenanbieter angeboten wird). Außerdem weigern sich einige Diensteanbieter, auf Nutzeranforderungen zur Löschung von Daten, und insbesondere von kompletten Profilen schnell (oder sogar überhaupt) zu reagieren.

2. *Der irreführende Begriff der „Gemeinschaft":* Viele Diensteanbieter geben an, dass sie Kommunikationsstrukturen aus der „realen Welt" in den Cyberspace übertragen. Eine häufige Aussage ist, es sei sicher, (personenbezogene) Daten auf diesen Plattformen zu veröffentlichen, weil es lediglich der Weitergabe an Informationen an Freunde (wie früher im direkten Kontakt) gleiche. Eine genauere Betrachtung von Eigenschaften einiger dieser Dienste bringt jedoch zutage, dass diese Parallele einige Schwächen hat, einschließlich dessen, dass der Begriff des „Freundes" im Cyberspace in vielen Fällen grundlegend von der hergebrachten Idee von Freundschaft abweicht, und dass eine

[5] Bereits jetzt scheinen Geheimdienste in den Vereinigten Staaten von Amerika (insbesondere das „Open Source Center", eine Dienststelle, die dem US-amerikanischen „Director of National Intelligence" zugeordnet ist) Daten aus sog. „öffentlichen Quellen" zu nutzen, die anscheinend unter anderem YouTube, aber auch soziale Mediendienste wie Myspace und blogs einschließen;
vgl. http://www.fas.org/blog/secrecy/2008/02/open_source_intelligence_advan.html [abgerufen am 7. Februar 2008]

Gemeinschaft sehr groß sein kann[6]. Wenn die Nutzer nicht offen darüber informiert werden, wie ihre Profilinformationen weitergegeben werden und wie sie diese Weitergabe kontrollieren können, könnten sie durch die Idee der „Gemeinschaft", wie sie oben beschrieben ist, dazu verführt werden, gedankenlos personenbezogene Daten weiterzugeben, die sie sonst nicht weitergeben würden. Schon die Namensgebung mancher dieser Plattformen (z. B. „MySpace") erzeugt die Illusion von Intimität im Internet.

3. *„Kostenlos" ist vielleicht nicht „umsonst"*, wenn Nutzer vieler sozialer Netzwerke tatsächlich mit der zweckfremden Nutzung ihrer persönlichen Profildaten durch die Diensteanbieter „bezahlen", z. B. für (zielgerichtete) Werbung.

4. *Die Speicherung von Verkehrsdaten durch Anbieter sozialer Netzwerkdienste,* die technisch in der Lage sind, jede einzelne Bewegung eines Nutzers auf ihrer Website zu speichern; die eventuelle Weitergabe personenbezogener (Verkehrs-) Daten (einschließlich der IP-Adressen von Nutzern, die in manchen Fällen zusätzlich auch Aufenthaltsinformationen darstellen können) an Dritte (z. B. für Werbung oder sogar zielgerichtete Werbung). Es ist zu beachten, dass die Daten in vielen Rechtssystemen auch an Strafverfolgungsbehörden und/oder (nationale) Geheimdienste auf deren Verlangen weitergegeben werden müssen, unter Umständen sogar einschließlich ausländischer Stellen im Einklang mit existierenden Regelungen zur internationalen Kooperation.

5. *Die wachsende Notwendigkeit, Dienste zu refinanzieren und Gewinne zu erzielen, könnte die Erhebung, Verarbeitung und Nutzung von Daten der Nutzer weiter anheizen,* wenn und soweit diese den einzigen Vermögenswert der Anbieter sozialer Netzwerkdienste darstellten. Soziale Netzwerkwebseiten sind nicht – wie vielleicht der Ausdruck „sozial" nahe legen könnte – öffentliche Versorgungsbetriebe. Gleichzeitig wird Web 2.0 als Ganzes „erwachsen" und es gibt einen Wechsel von startups, die manchmal von Studentengruppen mit weniger finanziellen Interessen geführt werden, zu großen internationalen Unternehmen, die sich an diesem Markt beteiligen. Dies hat zu einer teilweisen Veränderung der Spielregeln geführt, weil viele dieser Unternehmen, die an nationalen Aktienbörsen notiert sind, unter einem extremen Druck ihrer Investoren stehen, Gewinne zu erzielen und zu maximieren. Weil für viele Anbieter sozialer Netzwerke die Daten in den Nutzerprofilen und die Nutzeranzahl (in Kombination mit der Nutzungshäufigkeit) den einzigen wirklichen Verkehrswert darstellt, den diese Unternehmen haben, könnte dies zu zusätzlichen Gefahren der unverhältnismäßigen Erhebung, Verarbeitung und Nut-

[6] Während einige Diensteanbieter versucht haben, begrenzte Bereiche innerhalb ihrer Dienste zu schaffen, um den Nutzern mehr Kontrolle darüber zu geben, wie sie ihre (personenbezogenen) Daten weitergeben, machen andere solche Informationen oder Teile davon einem größeren Publikum verfügbar, das in manchen Fällen in der gesamten Gemeinschaft bestehen kann – und damit in Millionen von völlig Fremden: „Zwar bleibt es unter uns", aber „wir" können durchaus mehr als 50 Millionen sein.

zung personenbezogener Daten der Nutzer führen. Dabei ist auch zu beachten, dass viele Anbieter sozialer Netzwerke das Konzept der Externalisierung von Kosten des Datenschutzes hin zu den Nutzern verfolgen[7].

6. *Es könnten mehr personenbezogene Informationen weitergegeben werden als man denkt:* So könnten z. B. Fotos zu universellen biometrischen Identifikatoren innerhalb eines Netzwerks oder sogar über Netzwerke hinweg werden. Software zur Gesichtserkennung ist in den letzten Jahren dramatisch verbessert werden und wird in der Zukunft sogar noch „bessere" Ergebnisse erzielen. Es ist zu beachten, dass, wenn einmal ein Name zu einem Bild hinzugefügt werden kann, dies auch die Privatsphäre und Sicherheit anderer, möglicherweise pseudonymer oder sogar anonymer Nutzerprofile in Gefahr bringen kann (z. B. bei Profilen in Kontaktanzeigen, die normalerweise aus einem Bild und Profilinformationen bestehen, aber nicht den wirklichen Namen des Betroffenen veröffentlichen). Die Europäische Netzwerks- und Informationssicherheitsagentur weist außerdem auf eine in der Entwicklung befindliche Technologie namens „content based image retrieval" (CBIR) hin, die weitere Möglichkeiten zur Lokalisierung von Nutzern durch Vergleich identifizierender Bestandteile eines Ortes mit Aufenthaltsinformationen in einer Datenbank ermöglicht[8] (z. B. ein Bild, das in einem Raum an der Wand hängt, oder ein abgebildetes Gebäude). Darüber hinaus führen „soziale Graphen"-Funktionen, die bei vielen sozialen Netzwerkdiensten beliebt sind, zur Offenlegung von Daten über die Beziehungen zwischen verschiedenen Nutzern.

7. *Missbrauch von Profildaten durch Dritte:* Dies ist möglicherweise das wichtigste Bedrohungspotenzial für personenbezogene Daten, die in Nutzerprofilen sozialer Netzwerkdienste enthalten sind. Abhängig davon, ob (Standard-) Einstellmöglichkeiten zum Datenschutz existieren und ob und wie diese von den Betroffenen genutzt werden, wie auch von der technischen Sicherheit eines sozialen Netzwerkdienstes, werden Profilinformationen, einschließlich Bildern (die den Betroffenen selbst, aber auch andere Personen abbilden können) im schlimmsten Fall der gesamten Nutzergemeinschaft zugänglich gemacht. Gleichzeitig existieren gegenwärtig nur sehr wenige Schutzvorkehrungen gegen das Kopieren von Daten jeglicher Art aus Nutzerprofilen und deren Nutzung zum Aufbau von Persönlichkeitsprofilen, und/oder deren Wiederveröffentlichung außerhalb des sozialen Netzwerkdienstes[9].

---

[7] vgl. die Rede von John Lawford (Canadian Public Interest Advocacy Center) beim OECD-Canada Technology Foresight Forum „Confidence, privacy and security" am 3. Oktober 2007; http://www.stenotran.com/oecd/2007-10-03-Session4b.pdf [abgerufen am 6. Februar 2008], S. 35

[8] vgl. ENISA Position Paper No. 1: „Security Issues and Recommendations for Online Social Netzworks", October 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

[9] Dabei ist zu beachten, dass einige soziale Netzwerkdienste es Suchmaschinen gestatten, Daten ihrer Nutzer zu durchsuchen und dass in letzter Zeit Suchmachinendienste entstanden sind, die auf das Angebot von Persönlichkeitsprofilen spezialisiert sind, die aus verschiedenen Quellen zusammengestellt werden. Andererseits scheinen Diensteanbieter gegenwärtig wenig oder sogar überhaupt keine Kontrolle über die Handlungen von „Spidern" auf ihren Websites zu haben, die das „robots.txt"-Protokoll nicht respektieren.

Aber sogar die „normale“ Nutzung von Profildaten kann das informationelle Selbstbestimmungsrecht von Nutzern und beispielsweise auch ihre beruflichen Perspektiven in gravierender Weise beeinträchtigen[10]: Ein Beispiel, das öffentliche Aufmerksamkeit erlangt hat, ist die Durchsuchung von Nutzerprofilen von Bewerbern oder Angestellten durch Personalmanager, die sich als Standardprozedur zu entwickeln scheint: Presseberichten zufolge geben bereits heute ein Drittel aller Personalverantwortlichen an, für ihre Arbeit Daten aus sozialen Netzwerkdiensten zu nutzen, z. B. zur Überprüfung und/oder Vervollständigung von Bewerberdaten[11], Strafverfolgungsbehörden und Geheimdienste (einschließlich solcher aus weniger demokratischen Staaten mit niedrigen Datenschutzstandards) stellen weitere Instanzen dar, die wahrscheinlich Nutzen aus diesen Quellen ziehen werden[12]. Darüber hinaus stellen einige Anbieter sozialer Netzwerkdienste Nutzerdaten über Programmierschnittstellen Dritten zur Verfügung, so dass diese Daten sich dann unter der Kontrolle dieser Dritten befinden[13].

8. *Die Arbeitsgruppe ist besonders besorgt über* weiter steigende Risiken des Identitätsdiebstahls, die durch die breite Verfügbarkeit personenbezogener Daten in Nutzerprofilen und durch die mögliche Übernahme von Profilen durch nicht autorisierte Dritte gefördert werden könnten[14].

9. *Nutzung einer bekanntermaßen unsicheren Infrastruktur:* Viel ist bereits über den Mangel an Sicherheit von Informationssystemen und -netzen einschließlich Internetangeboten geschrieben worden. Zwischenfälle neueren Datums

---

[10] „26. April – Eine Frau aus Pennsylvania gibt an, dass ihre Laufbahn als Lehrer durch die Universitätsverwaltung aus dem Gleichgewicht gebracht worden ist, durch unfaire Disziplinarmaßnahmen wegen eines Fotos auf MySpace, das sie mit einem Piratenhut zeigt, wie sie aus einer Plastiktasse trinkt. In einem Bundesgerichtsverfahren gibt […] an, dass die Millersville Universität sie beschuldigt, für Alkoholkonsum Minderjähriger zu werben, nachdem sie ihr MySpace Foto entdeckt hatten, das mit ‚betrunkener Pirat‘ beschriftet war“. Zitiert aus http://www.thesmokinggun.com/archive/years/2007/0426072pirate1.html [abgerufen am 11. Februar 2008].
Vgl. auch „The Guardian“ vom 11. Januar 2008: „Would-be students checked on Facebook“; http://education.guardian.co.uk/universityaccess/story/0,,2238962,00.html

[11] Vgl. z. B. „Employers Use ‚Facebook‘ and ‚MySpace‘ to Weed Out Applicants“;
http://www.wtlv.com/tech/news/news-article.aspx?storyid=644533 [abgerufen am 12. Februar 2008]. Finnland scheint bisher das einzige Land zu sein, das solche Praktiken verbietet.

[12] Andere Beispiele, die sich in der Zukunft entwickeln könnten, könnten auch die Nutzung durch Einwanderungsbehörden bei Auslandsreisen einschließen.

[13] Vgl. z. B. „Facebook API Unilaterally Opts Users Into New Services“, von Ryan Singel, 25. Mai 2007, http://blog.wired.com/27bstroke6/2007/05/facebook_api_un.html; vgl. auch Chris Soghoian: „Exclusive: The next Facebook privacy scandal“, 23. Januar 2008,
http://www.cnet.com/8301-13739_1-9854409-46.html?tag=blog.1 [abgerufen am 12. Februar 2008]

[14] Vgl. als ein aussagekräftiges Beispiel z. B. die kürzlichen „Natalie“- und „frog“-Experimente, die von der Sicherheitsfirma Sophos durchgeführt worden sind; s. „Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves. Research highlights dangers of irresponsible behaviour on social networking sites“, August 2007;
http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html und „Der Fall ‚Natalie‘. Online Communities zunehmend IT-Sicherheits-Risiko. Experten warnen vor massivem Anstieg von Datendiebstahl und -missbrauch auf Social Network Websites“, 21 Januar 2008

betreffen auch bekannte Anbieter sozialer Netzwerke wie Facebook[15], flickr[16], MySpace[17], Orkut[18] und den deutschen Anbieter „StudiVZ“[19]. Obwohl die Diensteanbieter Maßnahmen zur Verbesserung der Sicherheit ihrer Systeme getroffen haben, gibt es hier immer noch Möglichkeiten zur weiteren Verbesserung. Gleichzeitig ist es wahrscheinlich, dass auch in Zukunft neue Sicherheitslücken auftauchen werden und es ist aufgrund der Komplexität der Softwareanwendungen auf allen Ebenen von Internetdiensten[20] unwahrscheinlich, dass 100%ige Sicherheit jemals realisiert werden kann.

10. *Ungelöste Sicherheitsprobleme von Internetdiensten* tragen zu den Risiken der Nutzung sozialer Netzwerkdienste bei und könnten in bestimmten Fällen solche Risiken verstärken oder zur Entwicklung von spezifischen Spielarten dieser Risiken für soziale Netzwerkdienste führen. Ein kürzlich veröffentlichtes Positionspapier der Europäischen Netzwerk- und Informationssicherheitsagentur (ENISA) benennt u. a. SPAM, cross site scripting, Viren und Würmer, spear-phishing und Phising (spezifisch für soziale Netzwerke), die Infiltrierung von Netzwerken, Profil-Übernahmen und Rufschädigungen durch Identitätsdiebstahl, Stalking, Mobbing und Wirtschaftsspionage (d. h. social engineering-Angriffe unter Nutzung von sozialen Netzwerkdiensten[21]). Nach Aussage von ENISA stellen Aggregatoren für soziale Netzwerke („social network aggregators“) ein zusätzliches Sicherheitsrisiko dar[22].

11. *Die Einführung von Interoperabilitätsstandards und Anwendungsprogrammierungs-Schnittstellen* (Application Programming Interfaces – API; z. B. „open social“, das von Google im November 2007 vorgestellt wurde), um ver-

---

[15] Vgl. „Secret Crush Facebook App Installing Adware, Security Firm Charges“, „Wired“ vom 3. Januar 2008, http://blog.wired.com/27bstroke6/2008/01/secret-crush-fa.html [abgerufen am 12. Februar 2008]

[16] Vgl. „Phantom Photos: My photos have been replaced with those of another“; http://flickr.com/help/forum/33657/ [abgerufen am 12. Februar 2008]

[17] Vgl. z. B. im Dezember 2006 „MySpace XSS QuickTime Worm“; http://www.websense.com/securitylabs/alerts/alert.php?AlertID=708 [abgerufen am 12. Februar 2008]

[18] Vgl. PC World: „Worm Hits Google's Orkut“ vom 19. Dezember 2007, http://www.pcworld.com/article/id,140653-c,worms/article.html, und SC Magazine US: „cGoogle's Orkut hit by self-propagating trojan“ vom 26. Februar 2008, http://www.scmagazineus.com/Googles-Orkut-hit-by-selfpropagating-trojan/article/107312/ [beide abgerufen am 3. März 2008]

[19] vgl. „Datenleck beim StudiVZ? [Update]“; http://www.heise.de/newsticker/meldung/81373/ [abgerufen am 12. Februar 2008]

[20] Außerdem wird der jährliche steile Anstieg der Menge elektronisch gespeicherter Informationen selbst als ein Sicherheitsrisiko angesehen: Bei der letzten RSA Europe Security Conference in London im Jahr 2007 wurde der RSA-Präsident Art Coviello mit der Aussage zitiert, dass allein im Jahr 2006 weltweit 176 Exabytes an Daten generiert worden seien und dass eine solch riesige Menge von Daten aus seiner Sicht nicht verwaltbar sei und nicht effektiv gesichert werden könnte; vgl. das deutsche Computermagazin „iX“, Dezember 2007, S. 22: „Trübe Aussichten: Große Datenmengen verhindern Datensicherheit“; http://www.heise.de/kiosk/archiv/ix/2007/12/022/ [abgerufen am 12. Februar 2008]

[21] ENISA Position Paper No.1: „Security Issues and Recommendations for Online Social Networks“, Oktober 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

[22] vgl. ENISA Position Paper No.1 (s. Fußnote 21), S. 12

schiedene soziale Netzwerkdienste technisch interoperabel zu machen, enthalten zusätzliche neue Risiken: Sie erlauben die automatische Auswertung aller sozialen Netzwerke, die diesen Standard implementieren. Die API liefert buchstäblich die gesamte Funktionalität zur automatischen Auswertung, die auch in der Web-Schnittstelle implementiert ist. Mögliche Anwendungen, die das Potenzial für Rückwirkung auf die Privatsphäre der Nutzer haben (und möglicherweise auch für die Privatsphäre von Nicht-Nutzern, deren Daten Teil eines Nutzerprofils sind) könnten beinhalten: Die globale Analyse von (beruflichen und privaten) Nutzerbeziehungen, die sehr wohl „Grenzen" zwischen verschiedenen Netzwerken überschreiten können, in denen Nutzer in verschiedenen Rollen agieren (z. B. beruflich orientierte gegenüber mehr freizeitorientierten Netzwerken). Interoperabilität könnte auch das Herunterladen und die Verwendung von Profilinformationen und Fotos durch Dritte fördern, sowie die Erstellung von Aufzeichnungen über Veränderungen in Nutzerprofilen (einschließlich des Verfügbarmachens von Informationen, die ein Nutzer aus seinem Profil gelöscht hat).

Empfehlungen

Gestützt auf das oben Gesagte gibt die Arbeitsgruppe die folgenden (vorläufigen) Empfehlungen für Gesetzgeber, Anbieter und Nutzer von sozialen Netzwerkdiensten:

Gesetzgeber

1. *Einführung eines optionalen Rechts auf pseudonyme Nutzung – d. h. in einem sozialen Netzwerkdienst unter einem Pseudonym zu handeln*[23] – wo dies nicht bereits Teil des Regulierungsrahmens ist.

2. *Es muss sichergestellt werden, dass Diensteanbieter in ehrlicher und klarer Weise darlegen, welche Daten für den Basisdienst erforderlich sind, so dass die Nutzer eine informierte Wahl treffen können, ob sie den Dienst in Anspruch nehmen wollen,* und dass Nutzer jegliche zweckfremde Nutzung (wenigstens durch Widerspruch) ablehnen können, insbesondere zum Zwecke von (zielgerichteter) Werbung. Dabei ist zu beachten, dass hinsichtlich der Einwilligung von Minderjährigen besondere Probleme bestehen[24].

[23] „Pseudonyme Nutzung" bedeutet in diesem Kontext das Recht, in einem sozialen Netzwerkdienst unter einem Pseudonym zu handeln, ohne seine „wirkliche" Identität gegenüber anderen Nutzern des Dienstes oder der Öffentlichkeit offenbaren zu müssen, wenn der Nutzer dies wünscht. Abhängig von den konkreten Umständen, kann dies sehr wohl eine Verpflichtung zur Preisgabe der wirklichen Identität gegenüber dem Anbieter eines sozialen Netzwerks bei der Registrierung einschließen.

[24] vgl. das „Arbeitspapier zum Schutz der Privatsphäre von Kindern im Netz: Die Rolle der elterlichen Einwilligung", angenommen bei der 31. Sitzung der Arbeitsgruppe am 26./27. März 2002 in Auckland (Neuseeland); http://www.datenschutz-berlin.de/attachments/204/child_de.pdf?1177661067

3. *Einführung einer Verpflichtung für Anbieter sozialer Netzwerkdienste zur Benachrichtigung bei Sicherheitsvorfällen.* Nutzer sind nur dann in der Lage, insbesondere mit den steigenden Risiken von Identitätsdiebstahl umzugehen, wenn sie über jegliche Datensicherheitsvorfälle unterrichtet werden. Eine solche Maßnahme würde gleichzeitig dazu beitragen, ein besseres Bild darüber zu erhalten, wie gut Unternehmen Nutzerdaten sichern, und ihnen einen zusätzlichen Anreiz liefern, ihre Sicherheitsmaßnahmen weiter zu optimieren.

4. *Überdenken des gegenwärtigen Regulierungsrahmens im Hinblick auf die Verantwortlichkeit* in sozialen Netzwerkdiensten veröffentlichte personenbezogene Daten (insbesondere für personenbezogene Daten Dritter) mit Blick darauf, möglicherweise den Anbietern sozialer Netzwerkdienste ein Mehr an Verantwortlichkeit für personenbezogene Daten auf sozialen Netzwerk-Webseiten zuzuweisen.

5. *Verbesserung der Integration von Datenschutzkenntnissen im Bildungssystem.* So wie die online Veröffentlichung personenbezogener Daten Teil des täglichen Lebens besonders junger Menschen wird, müssen Datenschutz und Instrumente zum informationellen Selbstschutz Teil der Schul-Lehrpläne werden.

<u>*Anbieter von sozialen Netzwerkdiensten*</u>

Anbieter sollten ein vitales Eigeninteresse an der Datensicherheit und dem Schutz personenbezogener Daten ihrer Nutzer haben. Ein Versäumnis schneller Fortschritte in diesem Bereich könnte zum Verlust des Vertrauens der Nutzer (das bereits jetzt durch kürzliche Datenschutz- und Datensicherheitsvorfälle beträchtlich erschüttert ist) und damit sehr wohl zu einem ökonomischen Rückschlag führen, der mit der Krise vergleichbar ist, die die digitale Wirtschaft in den späten 90er Jahren erschütterte.

1. *Verständliche und offene Informationen der Nutzer* ist eines der bedeutendsten Elemente jeglicher fairen Verarbeitung und Nutzung personenbezogener Daten. Während die Notwendigkeit eines solchen Mechanismus in den meisten nationalen, regionalen und internationalen Regulierungsinstrumenten zum Datenschutz anerkannt ist, muss u. U. die gegenwärtige Form, in der viele Diensteanbieter ihre Nutzer informieren, erneut überdacht werden: Gegenwärtig – und in vielen Fällen im Einklang mit dem existierenden Regulierungsrahmen – stellen Informationen über den Datenschutz einen Teil von manchmal komplizierten und länglichen Vertragsbedingungen des Diensteanbieters dar. Zusätzlich wird manchmal eine Datenschutzinformation angeboten. Manche Diensteanbieter legen nahe, dass der Prozentsatz der Nutzer

sehr klein ist[25], die diese Informationen tatsächlich herunterladen. Selbst wenn diese Information dem Nutzer zum Zeitpunkt der Registrierung auf dem Bildschirm angezeigt wird und auf Wunsch des Nutzers auch später abgerufen werden kann, könnten dem Ziel der Information der Nutzer über mögliche Konsequenzen ihres Handelns während der Nutzung des Dienstes (z. B. bei der Veränderung von Datenschutz-Einstellungen einer Sammlung von Bildern) besser durch eingebaute, kontext-sensitive Funktionen gedient werden, die die angemessene Information auf der Basis der Handlungen der Nutzer liefern.

Die Nutzer sollten insbesondere Informationen über den Regulierungsrahmen enthalten, dem ein Diensteanbieter unterliegt, über ihre Rechte (z. B. auf Auskunft, Berichtigung und Löschung) im Hinblick auf ihre eigenen personenbezogenen Daten und zu dem Geschäftsmodell, das zur Finanzierung des Dienstes angewandt wird. Die Information muss auf die spezifischen Bedürfnisse der jeweiligen Zielgruppe zugeschnitten werden (besonders bei Minderjährigen), damit diese informierte Entscheidungen treffen können.

Die Information der Nutzer sollte sich auch auf den Umgang mit Daten Dritter beziehen: Anbieter sozialer Netzwerkdienste sollten – zusätzlich zur Information ihrer Nutzer über die Art und Weise, wie sie die Daten der Nutzer behandeln – auch über Ge- und Verbote im Hinblick darauf informieren, wie die Nutzer Daten Dritter behandeln dürfen, die in ihren Profilen enthalten sind (z. B. wann die Einwilligung eines Betroffenen vor der Veröffentlichung eingeholt werden muss oder über mögliche Konsequenzen von Regelverstößen). Besonders die riesigen Mengen von Fotos in Nutzerprofilen, auf denen Dritte abgebildet sind (in vielen Fällen sogar versehen mit Hinweisen auf den Namen und/oder das Nutzerprofil des Dritten) spielen in diesem Kontext eine Rolle, weil die gegenwärtigen Praktiken in vielen Fällen nicht mit den existierenden gesetzlichen Rahmen zur Regelung des Rechts am eigenen Bild übereinstimmen.

Freimütige Informationen sollten auch über verbleibende Sicherheitsrisiken gegeben werden und über andere mögliche Konsequenzen der Veröffentlichung personenbezogener Daten in einem Profil, wie auch über den möglichen gesetzmäßigen Zugriff durch Dritte (einschließlich Strafverfolgungsbehörden und Geheimdiensten).

[25] Ein Vertreter von Facebook erklärte kürzlich auf einer Konferenz der OECD, dass der Prozentsatz der Nutzer, die eine Datenschutzinformation abrufen, nicht höher als ein Viertel % sein könnte; vgl. http://www.stenotran.com/oecd/2007-10-03-Session4b.pdf, S. 33 f [abgerufen am 6. Februar 2008]

2. *Einführung der Möglichkeit, pseudonyme Profile zu erstellen und zu nutzen,* sowie deren Bewertung.

3. *Einhaltung von Versprechungen gegenüber den Nutzern:* Eine „conditio sine qua non" zur Förderung und zum Erhalt des Nutzervertrauens ist die klare und unmissverständliche Information darüber, wie ihre Daten durch den Diensteanbieter genutzt werden, besonders, soweit es die Übermittlung personenbezogener Daten an Dritte betrifft. Bei einigen Diensteanbietern bestehen allerdings gegenwärtig Zweideutigkeiten im Hinblick auf diese Versprechungen. Das bekannteste Beispiel ist die beliebte Aussage „Wir werden Ihre personenbezogenen Daten niemals an Dritte weitergeben" in Verbindung mit zielgerichteter Werbung. Während diese Aussage in den Augen des Diensteanbieters formal korrekt sein mag, unterlassen es manche Anbieter, in klarer Weise die Tatsache zu kommunizieren, das z. B. für die Anzeige von Werbeeinblendungen in dem Browser-Fenster eines Nutzers die IP-Adresse dieses Nutzers an einen anderen Diensteanbieter, der den Inhalt der Werbung liefert, weitergegeben werden könnte. Dies geschieht in manchen Fällen gestützt auf Informationen aus dem Profil eines Nutzers, die der Anbieter des sozialen Netzwerkdienstes verarbeitet. Während die Profilinformation selbst möglicherweise tatsächlich nicht an den Werbeanbieter weitergegeben wird, wird sehr wohl die IP-Adresse des Nutzers übermittelt[26] (falls der Anbieter des sozialen Netzwerks nicht z. B. einen Proxy-Mechanismus nutzt, um die IP-Adresse des Nutzers gegenüber dem Werbeanbieter zu verbergen). Einige Anbieter sozialer Netzwerkdienste nehmen irrtümlich an, dass es sich bei IP-Adressen nicht um personenbezogene Daten handelt, während dies in den meisten Rechtsordnungen tatsächlich der Fall ist. Solche Mehrdeutigkeiten können Nutzer irreführen, und eine Erosion des Vertrauens befördern, wenn die Nutzer erfahren, was wirklich passiert. Dies ist weder im Interesse der Nutzer, noch im Interesse des Diensteanbieters. Vergleichbare Probleme existieren hinsichtlich der Nutzung von Cookies.

4. *Datenschutzfreundliche Standardeinstellungen* spielen beim Schutz der Privatsphäre der Nutzer eine Schlüsselrolle: Es ist bekannt, dass nur eine Minderheit von Nutzern Veränderungen an Standardeinstellungen einschließlich der Datenschutzeinstellungen vornimmt, wenn sie sich bei einem Dienst anmelden. Die Herausforderung für die Diensteanbieter liegt dabei darin, Einstellungen zu wählen, die standardmäßig einen hohen Grad an Schutz der Privatsphäre bieten, ohne den Dienst unbenutzbar zu machen. Gleichzeitig ist die Benutzerfreundlichkeit der Einstellmöglichkeiten entscheidend dafür, die

[26] Abhängig von den Umständen kann der Werbeanbieter sogar in der Lage sein, einige oder die gesamte dahinterliegende Profilinformation auf der Basis der Art der zielgerichteten Werbung, die einem bestimmten Nutzer angezeigt werden soll, zu rekonstruieren.

Nutzer zu Änderungen zu ermutigen. In jedem Fall sollte die Nicht-Indexierbarkeit von Profilen durch Suchmaschinen als Standard eingestellt sein.

5. *Verbesserung der Nutzerkontrolle über die Nutzung von Profildaten:*

   - *Innerhalb der Gemeinschaft;* z. B. indem die Sichtbarkeit ganzer Profile und von in den Profilen enthaltenen Daten begrenzt werden kann, wie auch die Begrenzung der Sichtbarkeit in Bezug auf Suchfunktionen innerhalb des Netzwerks. Die Kennzeichnung von Fotos (d. h. das Hinzufügen von Links auf existierende Nutzerprofile oder des Namens der abgebildeten Person(en) sollte an die vorherige Einwilligung der Betroffenen gebunden sein.

   - *Schaffung von Möglichkeiten, die eine Kontrolle der Nutzer über die Nutzung von Profildaten durch Dritte erlauben* – dies ist unerlässlich, um insbesondere Risiken des Identitätsdiebstahls zu begegnen. Im Augenblick existieren allerdings nur begrenzte Möglichkeiten zur Kontrolle von Informationen, nachdem diese veröffentlicht sind. Die Erfahrungen der Film- und Musikindustrie mit Technologien zur digitalen Rechteverwaltung legt nahe, dass die Möglichkeiten in dieser Hinsicht auch in Zukunft begrenzt bleiben könnten. Trotzdem sollten Diensteanbieter Forschungsaktivitäten in diesem Bereich verstärken: Existierende und möglicherweise vielversprechende Ansätze sind u. a. Forschungsvorhaben zum „semantischen" oder „policy-aware web"[27], die Verschlüsselung von Nutzerprofilen, die dezentrale Speicherung von Nutzerprofilen (z. B. bei den Nutzern selbst), die Nutzung von Wasserzeichen-Technologien für Fotos, die Nutzung von Grafiken anstatt von Text für die Anzeige von Informationen und die Einführung eines Verfallsdatums, das Nutzer für ihre eigenen Profildaten setzen können[28]. Diensteanbieter sollten außerdem danach streben, die zweckfremde Nutzung insbesondere von Bildern zu verhindern, indem sie den Nutzern eine Funktion zur Verfügung stellen, die die Pseudonymisierung oder sogar Anonymisierung von Bildern ermöglicht[29]. Sie sollten dar-

---

[27] vgl. z. B. Daniel J. Weitzner, Jim Hendler, Tim Berners-Lee, Dan Connolly: Creating a Policy-Aware Web: Discretionary, Rule-based Access for the World Wide Web:, E. Ferrari and B. Thuraisingham (Herausgeber), Web and Information Security Idea Group Inc., Hershey, PA (in Erscheinen); http://www.w3.org/2004/09/Policy-Aware-Web-acl.pdf , und Sören Preibusch, Bettina Hoser, Seda Gürses und Bettina Berendt: Ubiquitous social networks – opportunities and challenges for privacy-aware user modelling; http://vasarely.wiwi.hu-berlin.de/DM.UM07/Proceedings/05-Preibusch.pdf [beide abgerufen am 12 Februar 2008].

[28] Vgl. z. B. The Royal Academy of Engineering: Dilemmas of Privacy and Surveillance. Challenges of Technological Change. März 2007, S. 40, Punkt 7.2.1

[29] vgl. ENISA Position Paper No.1: „Security Issues and Recommendations for Online Social Networks", Oktober 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf, S. 23

über hinaus effektive Maßnahmen zur Verhinderung des Durchsuchens und des massenweisen Herunterladens von Profildaten treffen. Insbesondere sollten Nutzerdaten durch (externe) Suchmaschinen nur dann durchsucht werden können, wenn der Nutzer seine ausdrückliche, vorherige und informierte Einwilligung gegeben hat.

- *Ermöglichung der Nutzerkontrolle über die zweckfremde Nutzung von Profil- und Verkehrsdaten;* z. B. für Werbezwecke, als Minimum: ein Widerspruchsrecht für allgemeine Profildaten, eine Einwilligung für sensitive Profildaten (z. B. politische Überzeugungen, sexuelle Orientierungen) und für Verkehrsdaten. Viele existierende Rechtsrahmen enthalten bindende Regelungen für die zweckfremde Nutzung für Werbezwecke, die von Anbietern sozialer Netzwerke eingehalten werden müssen. Sie sollten in Betracht ziehen, die Nutzer selbst darüber entscheiden zu lassen, welche ihrer Profildaten sie für zielgerichtete Werbung genutzt sehen wollen. Zusätzlich sollte die Einführung einer Gebühr nach Wahl des Nutzers als weitere Möglichkeit erwogen werden, um den Dienst dadurch, anstatt durch die Nutzung von Profildaten für Werbezwecke zu finanzieren.

- *Einhaltung der Rechte von Nutzern, wie sie in nationalen, regionalen und internationalen Rechtsrahmen zum Datenschutz anerkannt sind;* einschließlich des Rechts der Betroffenen auf zeitnahe Löschung ihrer Daten (dabei kann es sich auch um ganze Nutzerprofile handeln).

- *Berücksichtigung von Problemen, die im Falle der Übernahme oder des Zusammenschlusses von Unternehmen auftreten kann, die soziale Netzwerkdienste anbieten:* Einführung von Garantien für Nutzer, dass der neue Eigentümer gegenwärtige Datenschutz- (und Datensicherheits-)standards beibehält.

6. *Angemessene Mechanismen zur Behandlung von Beschwerden* sollten eingeführt werden (z. B. das „Einfrieren" angefochtener Informationen, oder von Bildern), wo diese nicht bereits existieren, sowohl für Nutzer sozialer Netzwerke, aber auch in Bezug auf personenbezogene Daten Dritter. Wichtig ist eine zeitnahe Rückmeldung an die Betroffenen. Maßnahmen könnten auch ein Bestrafungsmechanismus für missbräuchliches Verhalten in Bezug auf Profildaten anderer Nutzer und personenbezogene Daten Dritter beinhalten (einschließlich des Ausschlusses von Nutzern von einem Dienst, soweit es angemessen ist).

7. *Verbesserung und Erhaltung der Sicherheit von Informationssystemen.* Nutzung anerkannter Methoden („best practices") bei der Planung, Entwicklung und dem Betrieb sozialer Netzwerk-Anwendungen, einschließlich unabhängiger Zertifizierung.

8. *Entwicklung und/oder weitere Verbesserung von Maßnahmen gegen illegale Aktivitäten wie Spamming und Identitätsdiebstahl.*

9. *Angebot verschlüsselter Verbindungen für die Pflege von Nutzerprofilen, einschließlich gesicherter Anmeldeprozeduren.*

10. *Anbieter sozialer Netzwerke, die in verschiedenen Ländern oder sogar global handeln, sollten die Datenschutzstandards der Länder respektieren, in denen sie ihre Dienste anbieten.*

Nutzer sozialer Netzwerke

1. *Seien Sie vorsichtig.* Denken Sie noch einmal darüber nach, bevor personenbezogene Daten (besonders Name, Adresse oder Telefonnummern) in einem sozialen Netzwerk-Profil veröffentlicht werden. Denken Sie auch darüber nach, ob Sie mit diesen Informationen oder Bildern in einer Bewerbungssituation konfrontiert werden möchten. Pflegen Sie Ihre Profilinformation. Lernen Sie von Geschäftsführern großer Unternehmen: Diese Personen kennen den Wert ihrer personenbezogenen Daten und kontrollieren sie. Deswegen werden Sie keine großen Mengen personenbezogener Informationen über diese Personen im Netz finden.

2. *Denken Sie noch einmal darüber nach, bevor Sie Ihren echten Namen in einem Profil benutzen.* Nutzen Sie stattdessen ein Pseudonym. Bedenken Sie, dass Sie selbst dann nur begrenzte Kontrollmöglichkeiten darüber haben, wer Sie identifizieren kann, weil Dritte in der Lage sein könnten, ein Pseudonym aufzudecken, besonders auf der Basis von Bildern. Erwägen Sie die Nutzung verschiedener Pseudonyme auf verschiedenen Plattformen.

3. *Respektieren Sie die Privatsphäre anderer.* Seien Sie insbesondere vorsichtig bei der Veröffentlichung personenbezogener Daten über andere (einschließlich Bildern oder sogar Bildern mit Zusatzinformationen) ohne die Einwilligung dieser Person. Bedenken Sie, dass die rechtswidrige Veröffentlichung besonders von Bildern in vielen Rechtsordnungen eine Straftat darstellt.

4. *Informieren Sie sich:* Wer bietet diesen Dienst an? Innerhalb welchen Rechtsrahmens? Gibt es einen adequaten Rechtsrahmen zum Schutz der Privatsphäre? Gibt es eine unabhängige Aufsichtsinstanz (wie z. B. einen Datenschutzbeauftragten), an den Sie sich im Fall von Problemen wenden können? Welche Garantien gibt der Diensteanbieter im Hinblick auf den Umgang mit Ihren personenbezogenen Daten? Ist der Dienst von unabhängigen und vertrauenswürdigen Einrichtungen für einen guten Schutz der Privatsphäre, und für gute Sicherheit zertifiziert worden? Nutzen Sie das Internet, um sich über

die Erfahrungen anderer mit den Datenschutz- und Datensicherheitspraktiken eines Ihnen unbekannten Diensteanbieters zu informieren. Nutzen Sie vorhandenes Informationsmaterial von Anbietern sozialer Netzwerke, aber auch unabhängige Quellen wie Datenschutzbehörden[30], und Sicherheitsunternehmen[31].

5. *Nutzen Sie datenschutzfreundliche Profileinstellungen.* Begrenzen Sie die Verfügbarkeit von Informationen soweit wie möglich, insbesondere im Hinblick auf die Indexierung durch Suchmaschinen.

6. *Nutzen Sie andere Identifizierungsdaten* (z. B. Login und Passwort) als diejenigen, die Sie auf anderen Webseiten nutzen (z. B. für E-Mail oder zum Online-Banking).

7. *Nutzen Sie Kontrollmöglichkeiten* im Hinblick darauf, wie ein Diensteanbieter Ihre personenbezogenen Profil- und Verkehrsdaten verarbeitet. Widersprechen Sie beispielsweise der Nutzung für zielgerichtete Werbung.

8. *Achten Sie auf die Aktivitäten Ihrer Kinder im Internet,* insbesondere auf Webseiten sozialer Netzwerke.

Schlussbemerkung

Die Arbeitsgruppe fordert Verbraucherschutz- und Datenschutzorganisationen auf, angemessene Maßnahmen zu treffen, um Regulierer, Diensteanbieter, die Öffentlichkeit und insbesondere junge Menschen[32] auf Risiken für die Privatsphäre in Bezug auf die Nutzung sozialer Netzwerke und verantwortliches Verhalten bezüglich der eigenen personenbezogenen Daten, wie auch der Daten anderer, hinzuweisen.

Die Arbeitsgruppe wird zukünftige Entwicklungen bei sozialen Netzwerkdiensten im Hinblick auf den Schutz der Privatsphäre beobachten und diese Empfehlungen soweit notwendig überarbeiten und aktualisieren.

---

[30] vgl. z. B. die Broschüre „when online gets out of line“ , die gemeinsam von Facebook und dem Information and Privacy Commissioner von Ontario, Canada, veröffentlicht worden ist; http://www.ipc.on.ca/images/Resources/up-facebook_ipc.pdf, den Elternratgeber der amerikanischen Federal Trade Commission: „Social Networking Sites: A Parent's Guide“; http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec13.shtm und „Social Networking Sites: Safety Tips for Tweens and Teens“; http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm [alle abgerufen am 3. März 2008]

[31] vgl. z. B. die von Sophos für Facebook vorgeschlagenen Datenschutzeinstellungen; http://www.sophos.com/security/best-practice/facebook.html

[32] vgl. z. B. die Kampagne „dubestemmer“, die von der norwegischen Datenschutzbehörde gestartet worden ist; http://www.dubestemmer.no/english.php, das „DADUS“-Project der portugiesischen Datenschutzbehörde; http://dadus.cnpd.pt, und die in Fußnote 30 oben aufgeführten Initiativen

Empfehlung zur Umsetzung und Anwendung der Europaratskonvention Nr. 185 zur Computerkriminalität („Budapest Konvention“)

– Übersetzung –

Die Budapest Konvention von 2001 zur Computerkriminalität ist ein wesentliches Werkzeug zur internationalen Kooperation mit dem Ziel der Harmonisierung von Straftatbeständen, Strafverfahren und der gerichtlichen und polizeilichen Zusammenarbeit;

In Erwägung, dass verschiedenen Regelungen der Konvention und das dazugehörige Protokoll, wie im Jahr 2003 unterschrieben, direkten Einfluss auf die Verarbeitung personenbezogener Daten haben und dass es wichtig ist, Datenschutzprinzipien bei der Ratifizierung und Umsetzung dieser Bestimmungen in Betracht zu ziehen;

In Erwägung, dass die Bestimmungen der Konvention nicht ausschließlich auf Computerkriminalität anwendbar sind, sondern auch auf die Erhebung von Beweisen in elektronischem Format für jegliche Art von Vergehen, ob mithilfe eines Computersystems begangen oder nicht;

In Erwägung, dass bestimmte Entscheidungen, die auf nationaler Ebene bei der Ratifizierung der Konventionen getroffen werden, auch Effekte auf die internationale Kooperation haben, insbesondere im Hinblick auf Verfahren zur gegenseitigen Hilfeleistung;

In Erwägung, dass auf einige kritische Punkte in diesem Bereich schon während der vorbereitenden Arbeiten für die Konvention hingewiesen worden ist, u. a. durch diese Arbeitsgruppe[1] und durch die Artikel 29-Arbeitsgruppe (Stellungnahme 4/2001 vom 22. März 2001);

in Erwägung, dass verschiedene Länder die Konvention unterschrieben haben, und dass 22 davon sie bereits ratifiziert haben;

EMPFIEHLT die Arbeitsgruppe,

dass besondere Aufmerksamkeit gerichtet werden soll auf alle Implikationen für die Verarbeitung personenbezogener Daten und die Sicherungseinrichtungen für Bürgerrechte in jeglichem Instrumenten zur Ratifizierung der Konvention und des dazugehörigen Protokolls, oder in Verbindung mit deren konkreter Umset-

[1] Vgl. „Gemeinsamer Standpunkt zu Datenschutzaspekten des Entwurfs einer Konvention zur Datennetzkriminalität des Europarates“ (Berlin, 13./14. September 200): http://www.datenschutz-berlin.de/attachments/217/cy_de.pfd?1200656839

zung durch die zuständigen Untersuchungsbehörden, insbesondere im Hinblick auf Folgendes:

1. **(Verhältnismäßigkeit)** Das Prinzip der Verhältnismäßigkeit, wie es in verschiedenen Artikeln der Konvention niedergelegt ist, sollte bei allen Aktivitäten zur Strafverfolgung, die von den zuständigen Strafverfolgungsbehörden durchgeführt werden (z. B. Untersuchungen, Durchsuchungen, Beschlagnahmen, Festnahmen, Vernehmungen, Suche nach Beweismitteln) immer dann beachtet werden, wenn das Beweismittel auf einem oder durch ein elektronisches Werkzeug gesammelt werden soll;

2. **(Sicherheitsmaßnahmen für Rechte Dritter)** Immer wenn diese Untersuchungstätigkeit ausgeführt wird, sollte ihr Einfluss auf die Rechte Dritter, die Außenstehende in Bezug auf die untersuchten Fakten sind, mit äußerster Sorgfalt abgeschätzt werden;

3. **(Verantwortung des Unternehmens für Straftaten von Beschäftigten)** In Bezug auf die Umsetzung der Bestimmungen der Konvention über die Verantwortung juristischer Personen (Artikel 12), die eine Verantwortlichkeit juristischer Personen vorsieht, die Einzelpersonen beschäftigen, die für Straftaten verantwortlich gemacht werden, die im Einklang mit der Konvention vorgesehen sind, sollte in Erwägung gezogen werden, die entsprechenden Bestrafungen auch anzuwenden, wenn die betreffenden Straftaten in der nationalen Gesetzgebung zum Schutz personenbezogener Daten enthalten sind;

4. **(„Einfrieren" von Verkehrsdaten)** Die Instrumente zur Umsetzung der Regelungen der Konvention im Hinblick auf die beschleunigte Erhaltung gespeicherter Computerdaten und die teilweise Mitteilung von Verkehrsdaten (Art. 16 und 17) sollte auf der Basis der sorgfältigen Abwägung der Zweckbindungs- und Verhältnismäßigkeitsprinzipien selektiv angewandt werden, wobei auch die Sicherungsmaßnahmen in Betracht gezogen werden sollen, die durch einige Länder festgelegt worden sind, die eine Vorratsdatenspeicherung von Verkehrsdaten für Zwecke der Strafverfolgung vorsehen;

5. **(Nationale Zuständigkeit zur Untersuchung und Aufdeckung von Straftaten)** Um Opfern von Computerkriminalität einen erweiterten Schutz zu bieten, sollte die Ratifizierung der Konvention und/oder jegliche daraus folgenden regulatorischen Änderungen insbesondere auf nationaler Ebene, die Möglichkeit zur Aktualisierung des nationalen Rechts bieten, insbesondere der Bestimmungen, die in den Strafvorschriften und/oder der Strafprozessordnung enthalten sind, um so den Anwendungsbereich der nationalen Gerichtsbarkeit bei der Verfolgung solcher Straftaten auszuweiten, die unbestraft bleiben könnten, wenn die herkömmlichen Standards der Strafgerichtsbarkeit angewandt würden (Art des Verhaltens, Fakten etc.).

Die Arbeitsgruppe erkennt die spezielle Bedeutung internationaler Zusammenarbeit in diesem Bereich an und behält sich vor, weitere Initiativen zu ergreifen, um den Austausch von Informationen, die Überwachung der angemessenen Anwendung der Konvention und des Protokolls, und die weitestmögliche Harmonisierung regulatorischer Ansätze und Umsetzungspraktiken zu fördern.

B. Dokumente zur Informationsfreiheit

Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)

1. Entschließung der 16. Konferenz am 11. Juni 2008 in Saarbrücken

Transparenz in der Finanzverwaltung

Die Informationsfreiheitsgesetze nehmen die Finanzverwaltung nicht von ihrem Anwendungsbereich aus. Deshalb gilt auch hier: Die grundsätzliche Offenheit der amtlichen Informationen gilt, sofern nicht eine in diesen Gesetzen geregelte Ausnahme (z. B. das Steuergeheimnis) greift.

In der Vergangenheit haben verschiedene Finanzbehörden häufig einen Anspruch der Bürgerinnen und Bürger auf Einsicht in eigene Steuerunterlagen sowie Verwaltungsvorgänge in das Behördenermessen gestellt. Der Bundesgesetzgeber habe mit dem Erlass der Abgabenordnung das steuerliche Verfahren abschließend geregelt und dort durch „absichtsvolles Unterlassen“ bewusst auf eine Regelung verzichtet. Nachdem das Bundesverfassungsgericht mit seinem Beschluss vom 10. März 2008 (1 BvR 2388/03) den Anspruch auf Informationen aus der eigenen Steuerakte für verfassungsrechtlich geboten erklärt hat, ist diese Argumentation nicht mehr länger haltbar.

Nichts anderes kann für die Anwendung der Informationsfreiheitsgesetze gelten, die jedem Menschen einen Anspruch auf Zugang zu den bei öffentlichen Stellen vorhandenen Informationen sichern. Der Zugang zur Information und die Transparenz behördlicher Entscheidungen ist eine wichtige Voraussetzung für die effektive Wahrnehmung von Bürgerrechten.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert die Finanzverwaltungen des Bundes und der Länder auf, die Informationsfreiheitsgesetze anzuwenden und in ihren nachgeordneten Bereichen durchzusetzen.

2. Entschließung zwischen der 16. und 17. Konferenz (vom 30. Juni 2008)

Die Europäische Union braucht nicht weniger, sondern mehr Transparenz

Mit der Verordnung 1049/2001 ist erstmals allen Unionsbürgerinnen und -bürgern der freie Zugang zu Dokumenten der Europäischen Union eröffnet worden. Die Verordnung hat unmittelbare Wirkung in allen Mitgliedstaaten, so dass auch deutsche Behörden, bei denen solche Dokumente vorliegen, sie beachten müssen.

Die Europäische Kommission hat nun allerdings Vorschläge vorgelegt, die – neben marginalen Verbesserungen – zu einer drastischen Einschränkung des Zugangs zu europäischen Dokumenten führen würden. Sie plant, den Zugang zu Dokumenten der EU-Institutionen künftig nur noch dann zu gestatten, wenn sie entweder bereits einem bestimmten Empfängerkreis übermittelt oder „registriert" worden sind. Damit hätten die europäischen Behörden es selbst in der Hand, zu bestimmen, welche Dokumente sie herausgeben. Darüber hinaus sollen Informationen, die die EU-Institutionen von außen im Rahmen laufender Verfahren erhalten, auch nach deren Abschluss selbst dann unter Verschluss gehalten werden können, wenn an ihrer Offenlegung ein überwiegendes öffentliches Interesse besteht. Schließlich sollen die EU-Institutionen Dokumente geheim halten dürfen, die sie zur Vorbereitung von Entscheidungen nur einem bestimmten Kreis extern Beratender zugänglich gemacht haben.

Die Informationsfreiheitsbeauftragten in Deutschland sehen die Gefahr, dass bei einer Annahme dieser Vorschläge eine massive Einschränkung der gebotenen Transparenz des Handelns europäischer Institutionen die Folge wäre. Sie teilen die Kritik, die der Europäische Bürgerbeauftragte in seiner Stellungnahme gegenüber dem Ausschuss für Bürgerrechte, Justiz und Inneres des Europäischen Parlaments am 2. Juni 2008 geübt hat (Presseerklärung deutsch: http://ombudsman.europa.eu/release/de/2008-06-02.htm. Text der Stellungnahme nur englisch: http://www.ombudsman.europa.eu/letters/en/20080526-1.htm). Die deutschen Informationsfreiheitsbeauftragten fordern deshalb das Europäische Parlament und den Rat auf, den Vorschlägen der Kommission nicht zu folgen und stattdessen das Transparenzniveau bei den Institutionen der Europäischen Union spürbar zu erhöhen.

3. Entschließung der 17. Konferenz am 3./4. Dezember 2008 in Schwerin

Die neue Konvention des Europarats zur Informationsfreiheit so bald wie möglich unterzeichnen und ratifizieren!

Der Ministerausschuss des Europarats hat am 27. November 2008 den Entwurf einer Konvention über den Zugang zu amtlichen Dokumenten beschlossen. Mit ihrem Inkrafttreten wird die Konvention alle Vertragsstaaten verpflichten, jedem Menschen ein allgemeines Recht auf gebührenfreien Zugang zu Behördeninformationen einzuräumen, ohne dass dies begründet werden muss.

Es ist zu begrüßen, dass damit erstmals weltweit ein völkerrechtlich verbindlicher Vertrag zur Informationsfreiheit auf den Weg gebracht worden ist.

Jetzt ist die Bundesregierung aufgefordert, die Konvention so bald wie möglich zu unterzeichnen und dem Bundestag zur Ratifikation zuzuleiten, damit die Konvention schnell in Kraft treten kann. Die wenigen verbleibenden Bundesländer, die noch immer keine Informationsfreiheitsgesetze verabschiedet haben, müssen ihre Haltung jetzt dringend revidieren, damit die Bundesrepublik nicht zum Schlusslicht unter den Mitgliedstaaten des Europarats wird.